

ANYSEC 安全网关

使用说明书

版权所有:深圳市中科网威科技有限公司



声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。 其版权归深圳市中科网威科技有限公司所有。 未经本公司书面许可,本手册的任何部分不得以任何形式手段复制或传播。

NOTICES

Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 2009 -2012 by Anysec-Tech. Co., Ltd. All Right Reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without express written permission of Anysec Co., Ltd.

ANYSEC 是深圳市中科网威科技有限公司注册商标。所有其他商标均属于<mark>有关</mark>公司所有。



目	录
	_

第一章	5介绍	6
0 0 0	目的:	
第二章 ●	⁵ 产品说明 产品概述 · · · · · · · · · · · · · · · · · · ·	7
● 第三章	应用拓扑	9
● ● 第四章	连接	i 10
● ● 第五章	工具栏功能	12
第六章	5快速安装向导	: 14
第七章	5 WEB 配置管理 20	1
0	系统管理 20 ◇ 状态 20 ◇ 设置 23	
	 ◇ 管理员	
0	网络管理	
	◆ 路由	



	\diamond	DNS	37
	\diamond	DHCP	38
	\diamond	会话	41
	\diamond	链路	44
€	用	户管理	45
	\diamond	用户	45
	\diamond	用户组	46
	\diamond	RADIUS	47
	\diamond	LDAP (略)	48
	\diamond	POP3 (略)	48
	\diamond	TACACS+ (略)	48
0	防	火墙	48
	\diamond	策略	48
	\diamond	地址	50
	\diamond	服务	53
	\diamond	时间	55
	\diamond	地址转换	56
	\diamond	IP/MAC 绑定	57
٢	VP	N 管理	59
	\diamond	点点通	59
	\diamond	设备隧道管理	59
	\diamond	PPTP	66
	\diamond	IPSEC	67
	\diamond	SSL VPN	72
	\diamond	移动客户端	74
	\diamond	配置客户端	76
٢	行	为管理	80
	\diamond	定义行为管理策略	80
	\diamond	DNS 定义	82
	Ŷ	网页定义	85
	\diamond	文件定义	88
	\diamond	邮件审计	89



	\diamond	带宽控制		
		络监控	92	
	\diamond	定义监控规则	92	
	\diamond	监控选项		
	\diamond	流量监控(具体功能依产品型号不同而不同)	94	
	\diamond	DNS 监控		
	\diamond	网页监控		
	\diamond	邮件监控		
	\diamond	聊天监控		
	\diamond	P2P 监控		
	\diamond	娱乐监控	100	
	\diamond	FTP 监控	101	
		志审计	101	
	\diamond	系统日志	102	
	\diamond	防火墙日志	102	
	\diamond	VPN 日志	102	
	\diamond	日志配置	104	
第八	章	Console 配置		
	⊃ 连	接		
	⊃ 配	置电脑		
	⊃ 基	本配置	107	
第九	〕章		.常见问题解答	109
	⊃ 故	障处理流程	110	
附:	点点ì	通配置实例		
	⊃ 客	户背景介绍	112	
	● 总	部点点通管理平台配置	112	
	⊃ 分	支节点配置:	118	



第一章 介绍

欢迎使用 ANYSEC 网络安全产品,构筑企业安全上网环境。

ANYSEC 全系列产品提供多种可靠的网络安全技术增强企业网络的安全性,避免了网络资源的误用和滥用,帮助企业更有效的使用通讯资源的同时不会降低网络的性能。

⇒ 目的:

本手册提供 ANYSEC 安全网关系列产品的硬件使用安装和调试配置操作说明, 并随购买的产品一并附给用户。

● 版本:

适用设备型号: ANYSEC S 系列、M 系列以及 T 系列。(某些功能、显示略有不同)

● 适用对象:

本手册适用于购买我公司 ANYSEC 安全网关系列产品的用户。要求使用者必须具备一定的网络知识和 TCP/IP 基础知识,并且熟悉电子设备的使用和保护。



第二章 产品说明

● 产品概述

ANYSEC 安全网关系列产品是基于 Anysec OS(Linux)开发的安全智能网关产 品,具备网络行为管理、流量监控、邮件审计、防火墙、VPN、代理上网、上网认 证等多种功能。为用户提供全方位网络安全互联解决方案。

目前 ANYSEC 安全网关系列产品已经通过公安部计算机信息系列安全产品质量 监督检验中心检验,并且获得了防火墙和 VPN 安全专用产品销售许可证书。

◇ 面板视图(设备不同,视图略有不同)



图 2-1: 设备面板视图

	LAN 指示灯:局域网连接 LAN 状态指示	WAN 指示灯:
广域网连接 WAN	状态指示	
	System 指示灯:系统状态指示	Power 指示灯:
电源状态指示		
	WAN: 广域网接口	LAN: 局域网
接口		
	Console 口: 串口线配置接口	E 口: 支持自
定义接口		



● 应用拓扑

以深圳、北京、香港为例组建常见应用的 IP VPN 网络,使用 ANYSEC 安全网关的网络应用拓扑如下示:



图 2-1:设备应用拓扑图



第三章 产品安装

首次连接并准备配置 ANYSEC 设备时,请参照一下图示连接: 1. 单机环境下设备接线参考图:



图 3-1: 与单机连线图

2. 交换机环境下设备接线参考图



图 3-1: 与交换机连线图

Э 登陆

ANYSEC 安全网关系列设备缺省配置说明:

- ◇ LAN/E0 口缺省 IP: 192.168.0.99 缺省端口: 8080
- ◇ 缺省登陆账号: 用户名: admin 密码: anysec
- ◇ 将配置电脑和 ANYSEC 设备缺省 LAN IP 为同一个网段,例如: 192.168.0.88
- ◇ 在 IE 浏览器中访问: <u>http://192.168.0.99:8080</u> 即可进入登陆界面



第四章 基于 Web 的管理器

本章介绍有关 Anysec 设备基于 Web 管理器管理接口的功能。

通过运行 Internet 浏览器的任何计算机使用 HTTP 或一个安全的 HTTPS 连接, 您便 能够配置并管理 Anysec 设备。

默认的 HTTP 端口是 8080, 默认的 HTTPS 端口是 8443。

Anysec 设备基于 Web 的管理器界面图:

💩 🚳	YSEC		2 🔅 🕢 🛃
 系統管理 就素 就素 管理点 逆 希 工具 网络管理 用門管理 用門管理 所次者理 いが常者理 (行力管理 (日表書) (1) 	设备机: 型号: 计可证: 拉作版本: 移动室户铺颇本: 硬件版本: 系统即构画本: 系统应动时间: 系统运转模式: 系统已运行:	derice5 AATTER-#4100 正式脱牧中印建 20100120-38097800 Yet, 0 20100101-7006 Sec#EE W2, 0-001001 West Jan 20 14:12157 2010 Med./Wart#式 1 Ge 1 1 Ge 1	
ANVANC	管理员: when	产品型号: 00:00	Jan 20 14:12:37 2010

图 4-1: Anysec 设备 Web 管理界面

使用基于 Web 的管理器可以配置大部分的 Anysec 设置以及监控 Anysec 设备的状态。使用基于 Web 管理器进行的配置更改无需重新设置防火墙或中断服务便可以生效。 配置完成后,可以保存设置作为备用。所保存的配置在任何时间都可以恢复。



● 工具栏功能

基于 Web 管理器中右上角的工具栏可以访问 Anysec 设备几项重要的功能。

自导	快速安装向导功能
会 保存	配置保存功能
? 帮助	帮助功能
————————————— 退出	退出功能

● 主菜单功能

基于 Web 管理器左边类似 Out look 菜单风格的主菜单提供了 Anysec 设备的各种配置功能。

系统管理	提供了系统状态查看、系统设置、管理员操作、证书管理、系统
	维护等子功能。
网络管理	提供了安全区定义、网络接口管理、路由管理、DNS/DDNS、DHCP
	服务、会话管理和链路管理功能。
用户管理	提供了用户和用户组的管理,支持多种认证方式。
防火墙	提供配置防火墙访问控制策略。
VPN 管理	提供多种 VPN 服务。
行为管理	提供上网行为管理策略服务。
网络监控	提供上网监控服务。
日志审计	提供详细的设备日志功能。

(注:系统功能依设备型号不同而有所不同)



第五章 基于 CLI 的管理器

本章介绍有关 Anysec 设备基于 CLI 管理器管理接口的功能。

通过运行 TELNET 或 SSH 的任何计算机使用 TELNET 或一个安全的 SSH 连接, 您便 能够配置并管理 Anysec 设备。

默认的 TELNET 端口是 8023, 默认的 SSH 端口是 8022。

Anysec 设备基于 CLI 的管理器界面如下图:

*********	*********************************
* Wei	lcome to Anysec UFM System 🛛 😽
×	*
* Anysec-Net	twork (ShenZhen) Co., Ltd Copyright 🛛 *
******	*************************
Welcome adm:	in it is Wed Nov 11 15:52:13 CST 2009
admin@> #	
^	
behavior	Enter Behavior Module
cls	Clear the screen
diagnose	Enter the Diagnose Module
execute	Enter Execute Module
exit	Exit this CLI session
firewall	Enter Firewall Module
help	Display an overview of the CLI syntax
history	Display the current session's command line history
log	Enter Log Module
logout	Logout of the current CLI session
netmonitor	Enter Netmonitor Module
network	Enter Network Module
showall	Show current running configuration
system	Enter System Module
user	Enter User Module
vpn	Enter VPN Module
admin@> #	

图 5-1: 基于 CLI 的管理器界面图

基于 CLI 的管理器提供了专业级的设置管理平台,在安全性要求较高的应用中,可以通过设备串口登陆,通过 CLI 管理器来配置设备,避免了网络配置过程中的不



安全因素。



第六章 快速安装向导

本章是关于如何使用快速安装向导来配置 Anysec 设备的内容描述。

1、点击工具栏的快速安装向导按钮



图 6-1:快速安装向导界面

快速安装向导的目的是协助您通过最简单的方式将 Anysec 设备接入 Internet。 注意:如果您以前已对该设备进行了部分配置操作,然后又通过快速安装向导来重新 配置设备的话,您之前配置的所有信息将会无效。

2、设置许可证



图 6-2:许可证设置界面

Anysec 设备的许可证分为两种:测试许可证和正式授权许可证。 测试客户选择申请试用,试用时间一般为一到二周,当设备检测到试用时间已结



束时,将会在 web 界面上提示您许可证已过期。这时您需要联系您的设备提供商以获 取正式授权许可证。

正式客户先选择下载授权许可证申请,申请文件的后缀是 dlr,将该文件提交给 您的设备提供商,以获取正式授权许可证文件,然后点击导入授权许可证导入正式许 可证文件。

注意:如果您的设备提供商已经将正式授权许可证导入了设备时,您可以选择 "跳过"按钮,忽略该功能配置。

3、设置设备运转模式



图 6-3:设备运行模式设置界面

Anysec 设备通过快速安装向导能够支持路由/NAT 模式和透明模式两种接入方式, 用户可以根据自身网络拓扑选择设备的运转模式。

路由/NAT 模式:打开设备路由功能,作为网关使用。

透明模式:关闭设备路由功能,网桥模式。

4、修改管理员密码



Nur rese	修改管理员密码
• • •	旧密码 新密码 确认新密码
and a	上一步 下一步 難过

图 6-4:管理员密码修改界面

您可以通过该界面修改管理员 admin 的密码, Anysec 设备出厂时默认密码是 anysec。

5、设置网络接口

对于不同的设备型号,配置网络接口的数目是不同的。Anysec 设备将会要求您 对所有设备接口进行配置。

0.0	西	2置接口: 1an0	
	接口类型	非广城网	
6	工作模式	S BOITE SAS	1
3 - CA	TPittit	192.168.118.1	
	网络捕绢	255. 255. 255. 0	
and the second		T-h but	

图 6-5:网络接口配置界面(非广域网)

根据需求配置相关网络接口参数。例如:

选择接口类型为 **"非广域口",**工作模式为 "ROUTE", IP 地址为 "192.168.9.1", 网络掩码为 "255.255.255.0";



1	配置接口: war	10
接口类型	广域网	•
工作模式	C ROUTE @ NAT	
地址模式	⑦ 固定IP ● PP	Par 🕐 DHEP
ISF类型	电信	
用户名	mAzecgmäzec. ct	a.
密码		
DIS積量	INI .	
	上-歩 下-歩	
	接口类型 工作极式 地址模式 可学类型 用户名 密码 305覆盖	

图 6-6:网络接口配置界面(广域网)

根据需求配置相关网络接口参数。例如:

选择接口类型为 "广域口", 工作模式为 "NAT", 地址模式为 "PPPOE"。用户 名为当地 ISP 提供商提供的用户名, 密码为当地 ISP 提供商提供的密码, DNS 覆盖 则为不选择;

NAT: 广域网工作模式;

固定 IP: 光纤、城域网等固定 IP 广域网接入方式;

PPPOE: ADSL 等拨号接入广域网方式;

DHCP: 某些特殊上网环境用户, 自动获取运营商 IP 接入方式。

6、设置 DNS

Part /			
<u>ی</u>		设置设备DNS	
	主365服务费:	202, 96, 128, 166	
	从385圈务器:	202, 96, 134, 133	
	1	1-# T-#	
1/2.			

图 6-7: DNS 设置界面

配置主 DNS 服务器,根据当地实际 DNS 填写。(请咨询相关工程师或搜索您所在地



DNS 信息)

例如 深圳电信: 主 DNS 服务器: 202.96.134.133; 从 DNS 服务器: 202.103.96.112

7、设置 DHCP 服务器

0		配置DI	ICP	服务	齐器
	謝券費名 状态	96.			
	17范围 月結推時 野认同关	255, 255, 255, 0		-	
	DISI開約週 FIDE服务器 接口	wand			
1.	86	28800	T-4	Ð	SE int

图 6-8:DHCP 服务器设置界面

根据实际需求配置 DHCP 服务器,如果不需要 DHCP 服务器功能可以直接选择"跳过"。

DHCP: 自动分配 IP 地址功能。



8、设置点点通隧道参数

TYREC /	配	置点点通	遂道
~ *	设备名	shenzhen	1
	设备ID	1000	
	遭退密码 隧道障障寻址方式: ◎ 通过公网IP或H	••••••••	
	● 通过Apysedo西 新昭由人統社	5-454J	
12	上-#		裁过

图 6-9: 点点通隧道设置界面

当您的设备无需用到点点通自动隧道功能时,您可以选择"跳过"按钮忽略该 功能配置。

8、保存配置



图 6-10:快速安装配置保存界面



第七章 WEB 配置管理

● 系统管理

本章用于描述 Anysec 设备的系统状态查看、设置、访问管理、设备证书管理和设备 维护等功能。

◇ 状态

用户点击状态菜单,可以查看设备版本信息、系统资源消耗和设备功能配额。

● 版本信息

设备名:	device3	
<u>표</u> 력:	ANVSIR-MET00	
许可证:	正式模拟许可证	12
软件版本:	20100120-30099000	
移动客户铺版本:	V6.0	
硬件版本:	20100101-X86	
系统架构版者:	Sector V0.0-001001	
系统启动时间:	Wed Jan 20 14:12:37 2010	
系統這時模式:	(新田/NAT現式	
系统已运行;	1 (7) 2 (191) 21 (191	1)

图 7-1:版本信息界面

管理员可以通过版本信息界面查看当前 Anysec 设备的基本情况,例如设备名、 设备型号、许可证、软件版本、移动客户端版本、硬件版本、系统架构版本、系统 启动时间、系统的运转模式以及当前已运行时间。

说明: 许可证一栏存在如下几种情况:

1、 显示"正式授权许可证", 表示该 Anysec 设备里已经导入了正式授权



许可文件。

- 2、 显示"试用(过期日:年月日 时间 星期)",表示 Anysec 设备处于试用 状态以及到期的时间。
- 3、 显示"没有许可证", 表示当前 Anysec 设备没有许可证, 该状态下部 分功能不可用。
- 系统资源

다V: 2用:20.998	(14): 202 (14): 202 (14): 202
内存 己用: 87476 (5.65%)	受量: 903672 空闲1 616196 (90, 32%)
内存 -/+ buffers/cashe: 已用: 24196-2.68%)	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
虔収豊: 己用: 28523600 E4 42%)	島重: 48737280 (空闲: 22215680(45:588)
合情: 2月:1370.090	思盟: 300000 空闲: 299853 (99, 95%)

图 7-2:信息资源界面

显示系统当前 CPU、内存、虚拟盘及网络会话的情况。



● 功能及配额

要求信息	主动出来	No.	2000 - C
主爆绕	功能使快	载大数器	10.00
Construction of the	CANALEMO	下其後	県高県島には熊
系统管理	百利於資	具备	是因素臺西和約益
	NAX SHORE	高粱	关排员在soull的合数约备及常常靠加
网络管理	aid in	200000	最大并发育详细
	twommiking	用量	展出支持4400004(近中)能
	1245公正	甘香菜	基因者發展的結晶的觀
	EEFSIATE	王昌委	量需要排mesul证功能
用户管理	TACACIDATE	2016年 平県委 提出医時の1936年期 2016年 平県委 優良支持のALUF4年間 第8 4198 行政得許的人名中国家	
	(MIN)	4294	行许位置的防火增加制制
	RANKE:	具备	是古具甸土防山庙内能
	地址	林田田	徽称省加的地址对新新大群
	腰肉	未須創	影然出版的事务对教育大都
	村田	(1)(1)	10.43-5000011/0020010大约
防火爐	(2)(0,17	末限制	%的4系/图1920-5是HU12-39380.20
	古田高裕能中心	具备	是古典皇后与 进程者的和政王 尼在刘下太石委会 出现时候
	西古語	85/III	影響建立把出亞運動構成大的
	THEFT	+現象)	能相違立的非常能夠很大的
	1819	44	一日に「「「「「「「「「「」」」」「「「」」」」「「」」」「「」」」」

图 7-3:功能及配额界面

显示当前系统的所具备的功能及性能参数。



◇ 设置

用户点击设置菜单,可以对设备进行时间设置、配置双机热备的高可行性功能 配置和配置设备运转模式。

● 时间设置

inter inter	利利投票
388888	1 196 2no 23, promoter, 2054
HER JAR	年x回:北中、封港、姜塘、新加坡 -
	et 00 + 10 00 +
- GMSZ	Ħ Jan + Ⅲ 01 + 〒 2000 +
hbreite	and and the second s
	SHILENLARINE THE JOI TO HAVE NOT
· tarende	242
	27.2
	R±185
	AVIS U.S.

图 7-4:设备时间设置界面

用户可以手工设置 Anysec 设备的系统时间,也可以与 PC 机同步时间,还可 以与因特网上的时间同步服务器同步时间。

● **双机热备**(依产品型号而定,一般低端型号不具备该功能)

		TW/54	
1	E作模式	主要式	
1	C作橋口	£3	
	BRUIN MILLI	10.15.10.99	
	き身相母に	A	(1-255)
	在古状态:	10	
	朝外状态。	10	



序。

图 7-5: 双机热备设置界面

双机热备功能: 是用于提供设备高可靠性服务的一种功能,通常的做法是提供 2 台或者多台设备模拟成一个虚拟设备,对外提供一个 IP 地址,来提供网络服务。

工作模式: 分为**主模式和运转模式、主模式和备份模式**, 主模式是处于激活 状态下提供正常网络服务的模式, 而备份模式则是处于等待激活状态, 一旦主模 式的设备出现故障, 备份设备发现后, 就会主动接管网络服务。

工作接口:是指双机热备的服务是用于处理哪个网络接口的。

虚拟 IP 地址: 是双机热备模式下对外提供的统一的 IP 地址。

热备组号:是一组优先级,用于指定各个备份设备转换主模式的优先次

抢占状态:是用于指定是否抢占主模式,主动提供服务的状态。 **服务状态**:是用于指定双机热备服务功能是否激活的状态。

前间设置	部集热装	直動爆火	1.447	
		最新运转模式	装置	
	這時模式	斎魚/RAT模式	1.5	

● 运转模式

图 7-6:设备运行模式设置界面

Anysec 设备提供多种接入方式,可以支持路由/NAT 模式、透明模式和桥接 模式及混合模式。用户根据自身网络规划,在运作模式中选择合适的设备接入方



式。注:桥接模式和混合模式只有在中高端产品中才提供。



◆ 管理员

•

管理员

用户点击管理员菜单,可以对 Anysec 设备的访问控制进行设置。管理员可以 访问 Anysec 设备并配置其操作。在设备初始化安装完成后,默认的配置只有一个 用户名为 admin 的管理员账户,其初始默认密码为 anysec。通过连接到基于 Web 的管理器或 CLI,用户也可以配置更多的管理员具有权限的 Anysec 设备的配置的 管理访问。

MITERS.	25日 月2	黑 化學	
		新建物理局	
	管理机名称		
	玉彩		
	确认密码		
	可慎主机	0. 0. 0. 0/0. 0: 0: 0	
	时值主机》	\$. 0, 0, 0/0, 0, 0, 0	
	柯值主机3	0. 0. 0. 0/0. 0. 0. 0	
	収解	adain -	
	明世	BX 195	
	and the second second		

图 7-7:新建管理员界面

添加一个新的管理员,可以指定密码、信任的主机和访问管理权限。

● 权限

		100 m 10 m		
192 X		and the		
100				
	(1) 本純管理 本 和 和 管理 本 和 和 管理 本 和 和 管理 本 和 和 管理 本 和 和 管理 本 和 和 管理 本 和 和 一 本 和 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 前 一 一 本 本 本 一 本 本 一 一 本 一 一 一 本 一 本 一 本 一 本 一 本 一 本 一 本 本 一 一 本 一 一 一 本 一 一 一 本 一 一 一 一 一 一 一 一 一 一 一 一 一	- 秋本 - 電源員 - 位約 - 位約 - 工具	* @	

图 7-8:新建权限界面

Anysec 设备的各个功能模块具有权限控制功能,因此用户可以自定义权限



集合,然后赋予指定的管理员,提供设备的多用户多权限管理。

只读权限:只能对该模块进行浏览操作,无法进行新建、修改、删除等 功能操作。

> **读写权限**:能够对该模块进行新建、修改、删除及浏览等所有功能操作 **不可视权限**:无法在界面上看到该模块的任何信息。

● 设置

會理員	収録 留吉	里名単	
		设置	
	管理病口:		
	HTTP1	8080	
	HTTPS:	8443	
	TELMET :	8023	
	BSE:	8022	
	要录设置:		
	空间和超目生	300	e)
	认证邮时:	1800	8
	登录失败最大值:	3	决
		柳田	

图 7-9:设备管理端口和登录参数设置界面

在设置功能中,用户可以配置 Anysec 设备的各种管理端口和登录参数。 **空闲超时:**当管理员登录界面后多长时间间隔内没有对界面进行任何操作时,

> Anysec 设备将主动删除本次会话信息并退回到登录界面。默认值 为 300 秒。

- **认证超时:** 当 Anysec 设备具有访问 Internet 的 Web 认证功能时,若用户通 过 Web 认证功能认证上网后多长时间间隔内没有对 Internet 进行 任何新建连接的访问操作时, Anysec 设备将主动删除该用户的上 网许可,并在下次用户访问 Internet 时再次出现认证页面要求进 行身份认证。默认值为 1800 秒
- 登录失败最大值: 当管理员获非法用户通过 Web 或 CLI 对设备进行管理时, 若登录失败次数达到该值,该登录用户的 IP 地址将被加入黑名单 以避免重复尝试。



● 黑名单

管理员 校課	12.2	2.9	255010
IF地址		已经录失数次数	9976

图 7-10:设备登录黑名单列表

当非法用户尝试登陆设备,多次认证失败后,该用户所用的 IP 就会被加入 到黑名单中,需要管理员来解除。

◇ 证书

用户点击证书菜单,可以进行符合 X. 509 标准的数字证书的相关操作,产生证书请求、管理本机证书、导入其他证书、根证书管理、证书作废列表管理等等。



图 7-11:证书相关设置界面

● 证书签署请求

第三方证书签署申请表



- 本机证书
- 远端证书
- CA 证书

中高端设备自带 CA 平台

● 证书作废表

注意:该部分使用配置请详见《SecROS UKey 管理员手册》; 如需使用该功能,请联系我司技术工程师协助,技术热线:

0755-83658229, 13510693536 (24小时)



◆ 维护

用户点击维护菜单,可以进行设备的配置保存、备份和恢复等操作。

● 保存配置

保存配置	备份配置	恢复配置	关机与重启	
		保存系统配置		
点击下ī	面"确定"按钮, 您	将保存系统中的所	行配置信息 !	
		确定		

图 7-12:保存配置界面

保存系统的所有配置信息。

● 备份配置

保存配置	备份配置	恢复配置	关机与重启	
		备份系统配置		
		◎ 备份系统配置		
		🔘 备份点点通平台	ź	
		确定		

图 7-13:备份配置界面

备份配置包含两种功能的备份:

- 1、 备份系统配置
- 2、备份点点通平台(当设备具备点点通平台功能时)



● 恢复配置

保存配置	骨的配置	板目探逻	关机与重启
		恢复系统配	
◎数	費出厂设置		
の恢	夏系统配置:		
			刻范
② 依	夏点点通平台:		
			测范
		關定	

图 7-14:恢复系统配置界面

恢复配置包含三种功能的恢复:

- 1、恢复出厂设置
- 2、恢复系统配置
- 3、恢复点点通平台(当设备具备点点通平台功能时)
- 关机与重启



图 7-15:设备关机与重启界面

通过系统进行软重启或关机操作。



○ 网络管理

本章用于描述如何将 Anysec 设备配置到网络中作为网络安全设备生效。基本的网络 设置包括配置 Anysec 设备的接口与用户的网络连接、以及配置 Anysec 的 DNS、DDNS 等 设置。

♦ 安全区

使用安全区可以将相关联的接口划分为一个集合进行管理。安全区名称的定 义与防火墙策略有直接关系,所有防火墙策略都是基于安全区来进行配置及管理 的。用户可以在安全区列表中添加安全区,编辑及删除安全区。添加安全区时, 选择该区域所包含的接口成员。

13	安全区	城员	編輯
1	878	bbib bbree shree	2
2	VAS .	pppi pppi EZ EL	a.
3	1.15	80 81	2

图 7-16:安全区设置界面

令 接口

点击接口菜单,用户可以:

- 1、修改物理接口的属性
- 2、添加并配置 VLAN 子接口(一般低端产品不具备该功能)
- 3、添加接口别名

橋口	Sec. 1			-	
类型	播口名	IF/Rank	05/40	秋杰	調羅
物理描口	E1 (ppp0)	116.204 100 220/255 255 255 255	ping http https tainst ash anep	Q. 20	13 11
物穿根口	the (ppp1)	218.18.209.40/295.255.255.255	ging http kttps telnet ash mer-	Ý 📲	13.0
前時期日	Rt.	202 168 1 1/225 258 258 0	ping http https telnet sub map	Ý 着	ARD
物理接口	100	192. IAN EN 1/255 255 268 0	ping http https telnet sub unap	9 2	221
原婚期日	Brest.	192 100 00 1/255 256 255 255	ping http https tilnet aih mep	0	12
障碍地口	19585	127.0.0.1/258.0.0.0	ping http hitps tellnet sik soop	Ŷ.	12 12
開婚接口	10 ¹ p	192 148 100 1725 255 255 295	ping http https talast sub map	9	1
新报餐口	bri dpill	0.0.0.0/0.0.0.0		9 1	100



图 7-17:接口状态界面

接口类型分为物理接口、隧道接口和桥接接口等多种。 点击修改按钮,可以修改接口的各种参数。如下图示:

搵口名	E2 (00:E0	±46¢74¢10;	10)		
撥口类型	广城网				
工作模式	C BOUTE	· BAT			
地址模式	● 固定IP	· FFP of	O DHCP		
LSP英型	电信				
用户名	anysec@1	63. ed			
密码					
005雜盖	ED.				
工作連军	自劫				
访问许可	SHMP		W HTTPS		
	V PING	W SSN	TELSET		
线路检测IP	-				Inable
动态域名				Enable	
安全级别	Ũ				
最大传输单元	1500				

图 7-18:接口设置界面

接口类型: 分为广域网接口和非广域网接口两种。当该接口所连网线与 Internet 直接连接时,一般选择"广域网";当该接口所连网线与您做在的内网直 接连接时,一般选择"非广域网"。

工作模式: 分为 ROUTE 模式和 NAT 模式。一般情况下,广域网接口选择 "NAT 模式",非广域网接口选择 "ROUTE"模式。

地址模式: ISP 提供的 Internet 接入模式, 依您的实际情况进行选择。

ISP 类型:目前提供有五种选择:电信、网通、铁通、联通或其他。这依您的实际情况进行选择。

DNS 覆盖: ISP 提供的 DNS 是否覆盖当前系统中的 DNS 配置信息。

线路检测 IP: 当您的设备存在多 WAN 链路时,您可以通过设置该检测 IP 以让设备进行自动检测链路是否正常。当设备检查到链路不通时将主动进行链路切



换。注: 该检测机制是通过 Ping 的方式进行的,请在填入检测 IP 时确认该 IP 地 址是否允许 Ping。

动态域名:当该接口与 Internet 连接后是否提供 DDNS 功能。若需要提供动态域名服务的功能,请先在 DDNS 中进行配置,然后在这里进行引用及可。

安全级别:当两个属于同一安全区的接口具有不同的安全级别时,防火墙将 从框架上保证来自安全级别高的接口的会话能够自由访问从安全级别低的接口出 去的连接,而无须添加任何防火墙策略,而来自安全级别低的接口的会话即使防 火墙的策略允许也不能访问从安全级别高的接口出去的连接。当两个属于同一安 全区的接口具有相同的安全级别时,需要添加防火墙的访问控制策略才能访问。

物理接口还可以提供 VLAN 功能(依具体产品型号而定,一般低端产品不具备 该功能)。

接口				
	新發	EVLAN接口		
	接口名			
	VLAN ID			
	接口类型	非广域网		•
	工作模式	ROUTE	🔘 NAT	
	IP地址			
	网络掩码			
	访问许可	🔽 SNMP	🔽 HTTP	🔽 HTTPS
		🔽 PING	🔽 SSH	V TELNET
	安全级别	0		T
	最大传输单元	1500		
	确定		取消	
			- MA	•

图 7-19: VLAN 接口设置界面

接口可以添加多个二级 IP。



接口	
新建排	轰口E1二级IP
IP地址	0. 0. 0. 0
网络掩码	255. 255. 255. 0
确定	取消

图 7-20:接口二级 IP 设置界面

◇ 路由

Anysec 设备提供静态路由和策略路由两种路由管理方式。出厂默认的配置下, Anysec 设备路由表只包含直连路由信息。用户可以通过定义其他的静态路由在路 由表中添加路由信息。

● 静态路由

下图为静态路由界面,用户可以查看设备当前的系统路由表,也可以通过添加按钮新增静态路由。

1	<mark>争态路由</mark>	略路由				
) (
ID	目的IP	子网掩码	网关地址	跳数	接口	编辑
1	192, 168, 118, 1	255, 255, 255, 255	0.0.0.0	0	ppsec0	
2	116, 204, 100, 1	255, 255, 255, 255	0.0.0.0	0	ppp0	
3	192, 168, 0, 99	255, 255, 255, 255	0.0.0.0	0	ppsec1	
4	218, 17, 59, 1	255, 255, 255, 255	0.0.0.0	0	ppp1	
5	192, 168, 118, 0	255, 255, 255, 0	0.0.0.0	0	ppsec0	
6	192, 168, 1, 0	255, 255, 255, 0	0.0.0.0	0	E1	
7	192, 168, 0, 0	255, 255, 255, 0	0.0.0.0	0	ppsec1	
8	192, 168, 59, 0	255, 255, 255, 0	0.0.0.0	0	EO	
9	127.0.0.0	255.0.0.0	0.0.0.0	0	ipsec	
10	0.0.0.0	0.0.0.0	116, 204, 100, 1	0	ppp0	
11	0.0.0.0	0.0.0.0	218, 17, 59, 1	0	ppp1	

图 7-21:静态路由设置界面



● 策略路由

每当一个数据包到达 Anysec 设备中任何一个接口时, Anysec 设备将通过使 用该数据包包头含代的源 IP 地址做逆向查询以识别该数据包是否在合法的接口接 收的。

如果 Anysec 设备通过接收该数据包的接口不能与计算机的源 IP 地址通信, 那么 Anysec 将丢弃该数据包。

如果目标地址与本地地址能够匹配(并且本地配置允许数据包的传输),那 么 Anysec 设备将数据包传送到本地网络中。

如果数据包的传输目的地是其他的网络, Anysec 设备根据路由策略或存储 在 Anysec 转发路由表中的信息将把数 据包转送在下一站中继路由。

当设置了路由策略并且数据包到达 Anysec 设备时, Anysec 设备根据策略路 由 表逐次查看并试图找到与该数据包相匹配的策略。如果发现匹配信息并且策略 中包含了足够的信息路由数据包(必须注明下一站路由的 IP 地址以及将数据包转 发的接口), Anysec 设备将使用策略中的信息路由数据包。如果 没有与数据包相 匹配的策略, Anysec 设备将使用路由表路由数据包。

静态路由	策略路由	
		新建策略路由
	如果数据包满足如	下条件:
	源IP/Mask	0. 0. 0. 0/255. 255. 255. 0
	目的IP/Mask	0.0.0/255.255.255.0
	协议	TCP 👻
	目的端口范围	
	将按以下方式处理	:
	输出接口	E3 🗸
	网关IP	0. 0. 0. 0
	确定	取消

下图为添加策略路由的操作界面。

图 7-22:新建策略路由设置界面


\diamond DNS

• DNS

Anysec 设备的 DNS 配置。一般该 DNS 服务器信息由 ISP 提供。

DNS	SecROS简域	DDNS		
		D	IS设置	
	主DNS服务器:	211.1	62.78.1	
	从DNS 脈旁音:	211.1	62.78.2	
		研	定	

图 7-23:DNS 设置界面

注意: 各地 DNS 并不相同, 请查询当地 ISP 运营商提供的 DNS 服务器信息。

● SecROS 简域

中科网威与 ISP 运营商合作,为客户提供的自主认证平台,非固定 IP 用户推荐使用该寻址模式。

设备寻址更加稳定、快速。该功能仅支持拥有点点通策略平台的设备。

BRS SecROSSING	1015	
	See	ROS資產發售
简诚名:		linzhouks
密码:		
确认密码:		
服葬状态:		



图 7-24: SecROS 简域设置界面

(默认出厂配置完成,如果因特殊原因导致丢失该信息,请联系中科网威工 程师重发配置信息)

• DDNS

Anysec 支持 DDNS(动态域名)功能。

下图为添加一个动态域名的操作界面。

NA2	See305期推	新建动木城名	
劫态	域名	anysec, 3322. org	
类型		qdns	
用户	8	anàisec	
密明		anyzec	

图 7-25:新建 DDNS 动态域名界面

目前 Anysec 设备只支持 3322 的动态域名服务, 您可以通过 http://www.3322.org 进行 DDNS(动态域名)免费申请,将相关信息输入以后, 在相关广域网接口的配置信息中选择您申请的 DDNS 即可,这样您就随时都能通过 DDNS 来对进行设备访问了。

♦ DHCP

DHCP 协议可以使 PC 自动获取分配的 IP 地址。或者也可以获取默认的网关与 DNS 服务器设置。一个 Anysec 物理接口或 VLAN 子接口能够提供以下 DHCP 服务:

- 1、为常规以太网连接提供常规的 DHCP 服务器服务。
- 2、为 IPSEC (VPN) 连接提供 IPSEC DHCP 服务器服务。
- 3、为常规以太网或 IPSEC 连接提供 DHCP 中继服务。

对于相同类型的连接(常规或 IPSEC),一个接口不能既提供 DHCP 服务器服务 又提供中继代理服务。 用户可以对任何 Anysec 接口配置 DHCP 服务器功能。DHCP 服务器对与该接口 连接的网络中的主机动态分配 IP 地址。在主机上必须配置使用 DHCP 自动获取分 配的 IP 地址。

如果一个接口通过路由器与多个网络连接,用户可以对每个网络添加一个 DHCP 服务器。每个 DHCP 服务器的 IP 地址范围必须与网络地址范围像匹配。路由 器必须配置使用 DHCP 中继代理。

Anysec 接口可以配置作为 DHCP 中继代理。接口将 DHCP 用户端的 DHCP 请求转 发到外部 DHCP 服务器并将回应返回到 DHCP 用户。DHCP 服务器必须具有适当的路 由,以便返回到 DHCP 用户的回应数据包能够到达 Anysec 设备。

● 服务器

RUN R	IF/BAC 即定	分配列表	unce-defit	6
CONTRACTOR OF THE		AN SEAMINE	57 6	
服务器名				
状态	1M			
IFDE		-		
网络撞码	255, 255, 255, 0			
默认同兴				
透名				
net BB 55 因	-	_		
VTNC82.55.55	-			
anua 1100/0022-68	1.00.00			
渡山	ppp1			
相視	28800	10		

下图为添加一个 DHCP 服务器的操作界面。

图 7-26:新建 DHCP 服务器界面

域名、DNS 服务器以及 WIS 服务器属于可选输入, 您可以依据您的具体情况进行填写。

● IP/MAC 绑定

该功能可以为具体的用户保留 IP 地址

根据用户设备 MAC 地址与连接类型、常规以太网连接或 IPSEC 连接;用户可



以为具体的用户保留一个 IP 地址。DHCP 服务器总是将保留的地址分配给该用户。

服务器	ER/MACHINE	分配列击	NICE-della
		新建DICF 1F/I	IAC供定
	名称		
	IF地址		
	MACHEN	_	
			-
	68 3	E	DC NB

图 7-27:新建 DHCP IP/MAC 绑定界面

● 分配列表

显示当前已分配的 IP 地址信息及过期时间等。



图 7-28:分配列表界面

● DHCP 中继

针对具有 DHCP 服务器的客户,提供 DHCP 中继服务。

國外國	17/MACHINE	新聞別式 経営1807中機能	smirshill.	
服务名 1012年	继接口	DBCP E1		
DHCT服 状态	务器口	192, 168, 59,	38	
	翻旋	10 11		
	WH ALL			



图 7-29:新建 DHCP 中继服务界面

◆ 会话

Anysec 设备提供会话和 ARP 查看,能够实时查看系统当前的网络会话状态、 ARP 信息和高级选项。

● 会话

显示当前设备的网络会话情况。

-	话	ARY I	鼎适喷			-		-	
18)台站S 掛袋	2017 - 54	逐端口	目的非	日的講	秋志	失效 (他)	授作	
1	339	10.0 0 2	SCILL	192, 168, 59, 1	0000	TIME_TAIT	115	1	
2	tep	10.0.0.2	92222	192.165.59.1	0000	ESTABLISHED	35999	-	
3.	tep	18.0.0.2	82205	192, 168, 59, 1	8080	TINE BOIT	115	1	
4	3 ep	10.0.0.2	\$2197	198, 168, 59, 1	0000	TIME_RAIT	114	179	
5	trep:	10.0.0.2	52218	192, 188, 59-1	peqe	TIME_BAIT	115	199	1
6	top	10.0.0.2	52204	192 168 57 1	néce	TIME_MAIT	115	19	
7	udy	211 182 101 114	14750	116 204 100 220	4466		14	199	1
8	timp.	10.0.0.2	52100	192.168.59.1	8080	TIME_NAIT	114	179	
0	step.	10.0.0.2	S2216	192.160.59.1	0000	TIME_WAIT	115 -	1	
10	tep	10.0.0 2	82193	192 168 56 1	RINED	TIME_RAIT	115	-	
								and the second s	1.00

图 7-30:当前设备的网络会话界面

• ARP

显示与当前设备接口连接的 ARP 信息,您可以通过通过"绑定状态"来将 PC 的 IP 和 MAC 进行绑定以抵御 Anysec 设备免受 ARP 欺骗攻击。注:当 PC 受到内网 ARP 攻击导致无法和 Anysec 设备通信时,请在您的 PC 上安装防 ARP 欺骗的杀毒软件来解决。





图 7-31:当前设备接口连接的 ARP 信息界面

● 高级选项

对 Anysec 设备的网络会话超时以及 TCP 会话数和 SYN 洪水攻击进行设置。

默认情况下 Anysec 设备的 TCP 会话的超时时间为 3600 秒; UDP 会话的超时时间为 30 秒; ICMP 会话的超时时间为 1 秒。

IP 最大 TCP 会话数限制: 对 PC 的并发 TCP 连接进行限制, 该功能能够在一定 程度上缓解 P2P 下载所造成的带宽滥用情况。

TCPMSS 设置:

入侵检测与防范: -

会话即时:		
TCP会话题时1	3600	秒
加强运动时	30	10
1009会话超时:	1	в
TCP高级选项:		
17最大117合运数探制:	U .	0表示不限制
TCFMSS设置1	0	0表示不识置
入层检测与防范:		
前ft2t洪水改击:	[3 7]	
TCF编口扫描攻击检测:	的	
ing/編日扫描攻击检测;	123	



∻

图 7-32:高级选项设置界面

WAN链路连接	WAN链路监控	
	(1) · · · · · · · · · · · · · · · · · · ·	
	设备的物理接口数重为: 4, 当前配置的\WAN口数重为: 3 您可以选择以下模式进行广域网互联:	
	● 单链路	
	◎ 多链路负载(会话)均衡	
	◎ 多链路备份	
	◎ 多链路负载(数据包)均衡	
	◎ 多链路负载 (IP)均衡	
	断线自动重联: ☑	
	确 定 重新连接 关闭连接	



链路

Anysec 设备提供链路管理及监控,支持多链路上网(低端设备无该功能)。

● WAN 链路管理

图 7-33: WAN 链路设置界面

当您的设备存在多 WAN 口配置时,您需要选择广域网联网模式为"多链路负载均衡"或"多链路负载均衡及带宽叠加",否则 Anysec 设备将按"单链路"进行联网处理。

		BPL/CH.	THE OCT	ULAWA.		PRO IN	OBIL		1000000
1 3	11	111.0	-		(10.000.000.000	(10.000.000.)	TRACTIONS	PETER	And 3m (8)
		10014	mat			IN 17.96's	coderer (he looote	100000 Temper 200	- 4nd Jun 10
									(thild and the

● WAN 链路监控

图 7-34:WAN 链路监控界面

对 WAN 联网情况进行监控, 能直观的显示接口的 WAN 连网方式, 当前 IP 地址、 网关地址、已发送和已接收的数据包及字节数以及改接口接入 Internet 的时间。



● 用户管理

配置用户验证

Anysec 设备验证设置是控制用户组的访问,但是创建用户组并不是配置验证的第一步。用户可以依据以下步骤配置用户验证设置:

如需要外部验证,可以配置 RADIUS、LDAP、POP3 或 TACACS 服务器。

进入"用户管理"->"用户",可以配置本地用户验证。对于每个用户,可以设 置通过 Anysec 设备、RADIUS 服务器、LDAP 服务器、POP3 服务器或 TACACS 服务器 校验密码。

◆ 用户

进入用户管理->用户,添加用户名称并配置验证。

下图为添加用户的操作界面。

AZ.	REENA	ACCESSION OF	
1.1. M 3	ERIPAR X	BUD W BURN	
U.	- E方式	• हत्त ाक्ताण्डांत्रेस ान्द्रात्रास्	
te E	认证选项: 验证订地址:	0.0.0.0	2
	1810年14月1日。 18月1日第二日 18月1日第二日日 18月1日第二日日日 18月1日第二日日日日 18月1日第二日日日日 18月1日第二日日日 18月1日第二日日日 18月1日第二日日日 18月1日第二日日日 18月1日第二日日日 18月1日第二日日日 18月1日第二日日 18月1日第二日日 18月11日 18月111 18月111 18月111 18月111 18月111 18月111 18月111 18月111 18月111 18月11 18月1111 18月111111 18月11111 18月111111 18月111111 181111 181111 181111 1	56	(司法)

图 7-35:新建认证用户界面

认证方式里面,支持多种认证,密码表示本地认证,其余部分均属于外部认证,需配置好对应的认证服务器。

Web 认证选项是用于上网认证的身份识别,可以绑定 IP 和 MAC 地址。

远程客户端接入指定 IP 是用于移动客户端接入的,如果填写了 IP 地址,则 使用该用户接入的远程客户端会分配指定的 IP。

状态表示该新建用户是否被激活启用。



◆ 用户组

一个用户组是一个或多个用户的集合。Anysec 设备出厂默认有三组用户组。

f Reblinth				
			w.,	2
2 MCListhe	66)	jaftīņo 王勤	L.	2
3 PPTPAuth				12

图 7-36:用户组显示界面

PPTPAuth 用户组:用于提供 PPTP 远程接入身份验证的用户组类型。

WebAuth 用户组:用于提供上网认证的身份验证的用户组类型。(默认组,不可改变)

MClientAuth 用户组:用于提供移动客户端远程接入身份验证的用户组类型。

注意:您在启用 PPTP 服务和移动客户端服务的时候可以选择 "PPTPAuth"认证用户组和 "MClientAuth"用户组,但也可以新建其他用户组,并将认证用户选入该用户组,在相关应用中引用就可以了。

WebAuth 用户组有点特殊,当您的防火墙策略需要用户进行 Web 认证上网的时候,请将用户加入该用户组,否则用户将无法认证上网。



用户组		
		编辑用户组
组名:	MClientAuth	
	可逃用户:	已逃用户:
Jeft IB	luo	
	68	定取期

图 7-37:编辑用户组界面

♦ RADIUS

对外部 Radius 服务器信息进行配置。

RADIN					
10	服务器名	IP地址	編口号	状态	

图 7-38:外部 Radius 服务器信息界面

新建 Radius 认证服务器:



KABL 写服务器			_
		新建RADIES认证服务器	
	服务器名		
	IFibid		
	180	1812	
	安全教教		
	対本	121	
	備定	IX #3	

图 7-39:新建 Radius 认证服务器界面

♦ LDAP (略)

♦ POP3 (略)

♦ TACACS+ (略)

服务器设置方法类似,如有疑问,请致电中科网威技术工程师: 0755-83658229。

● 防火墙

本章用于描述 Anysec 设备的防火墙功能,

Anysec 设备提供网络安全的核心功能都是围绕防火墙展开的,其上网行为管理和网络监控功能均需与防火墙策略的配合,管理员定义上网行为管理策略和网络监控策略,必须将其在防火墙策略中引用才能生效。

◇ 策略

防火墙策略控制所有通过 Anysec 设备的通信流量。添加防火墙策略控制 Anysec 安全区之间的连接与流量。

防火墙策略是 Anysec 设备决定如何处理连接请求的指令。当防火墙收到



一个数据包发出的连接请求时, Anysec 提取这个数据包的源地址、目的地址和服务(端口号)进行分析。

对于通过 Anysec 设备传输数据包,必须在 Anysec 设备上添加一个与该 数据包源地址、目的地址和服务相匹配的防火墙策略。该策略指导防火墙如 何处理这个数据包。处理方式可以是允许连接、拒绝连接、在连接前要求认 证,或将数据包作为 IPSec VPN 包处理。您也可以对防火墙策略添加日志记 录,配置 Anysec 设备记录对所有连接使用的策略。 防火墙通过对策略列表 的顺序搜索查找匹配策略。Anysec 设备的默认的策略是拒绝所有的连接。 策 略选项是通过创建或编辑防火墙策略时配置的。根据您所选择的不同的控制 方式,将呈现不同的策略选项。

		1 11 1 1								
	安全策略									
策										
略									状	
ID	包统计	源	目的	服务	时间	行为	监控	控制	态	编辑
	VPN -> VPN									
•	VPN -> WAN									
•	VPN -> LAN									
)	HAN -> VPN									
F 1	HAN -> WAN									
▶ 1	HAN -> LAN									Ľ
▶ 1	LAN -> VPN									Ľ
▶ 1	LAN -> WAN									
)	lan -> lan									

下图为防火墙策略列表的界面

图 7-40: 防火墙安全策略列表界面

添加防火墙策略:

点击插入策略按钮,可以添加一条安全策略。

安全策略的匹配条件包含了:

来源、流入接口、目的、流出接口、服务、时间、行为、控制、监控、流量 控制、日志、状态。

1、来源和目的对应防火墙地址;

2、服务对应防火墙服务;



- 3、时间对应防火墙时间;
- 4、行为对应行为管理的策略;
- 5、 控制包括运行、拒绝和认证,其中认证是指上网认证;
- 6、监控对于网络监控的策略;
- 7、流量控制包含启用和不启用两种状态;
- 8、日志标明是否记录数据包;
- 9、状态用于表明策略是否生效;

下图为插入安全策略的操作界面。

安全策略		
	插入安全策	information and the second
	来源	ANY -
	流入接口	ANY 👻
	目的	ANY 👻
	流出接口	ANY 👻
	服务	ANY 👻
	时间	ANY 👻
	行为	NONE -
	控制	ALLOW -
	监控	NONE -
	流量控制	disable 👻
	日志	
	状态	
	确定	取消

图 7-41: 插入安全策略设置界面

◇ 地址

用户可以根据需要添加、编辑以及删除防火墙地址。防火墙地址将被添加到 防火墙策略的源以及目标地址字段。添加到防火墙策略中的地址是用来与 Anysec 设备接收到数据包的源以及目标地址相匹配的。

● IP 掩码

一个防火墙地址可以是:

- 1、单个计算机的 IP 地址(例如, 192.168.0.69/255.255.255.255)。
- 2、一个子网的 IP 地址 (例如, class C 子网的地址 192.168.0.0/255.255.255.0)。



3、 0. 0. 0. 0/0. 0. 0. 0 表示所有可能的 IP 地址。 所添加的 IP 地址对应的掩码。例如:

▶ 单个计算机 IP 地址的掩码应该为 255. 255. 255. 255.

- ▶ Class A 子网的掩码应该为 255.0.0.0
- ▶ Class B子网的掩码应该为 255. 255. 0.0
- ▶ Class C 子网的掩码应该为 255. 255. 255. 0
- ▶ 所有地址的掩码应该为 0.0.0.0.0

注意: IP 地址为 0. 0. 0. 0 与掩码为 255. 255. 255. 255 不是有效的防火墙地址。

下图为新建 IP 掩码的操作界面。

17旗码 17范围 地址	
	新建工作推购
名称	
IF地址	0. 0. 0. 0
网络掩码	255, 255, 255, 0
状态	32
THE AT	TTU MR
00 12	0. H
4	

图 7-42:新建 IP 掩码设置界面

● IP 范围

IP 范围能够定义一段 IP 地址(如: 192.168.0.1 到 192.168.0.10)



IF推码	12.前间 地址组	
	3	R-B-1920H
	名称	
	起始IP	0. 0. 0. 0
	结束IP	0.0.0.0
	状态	1921
	8 2	EX VA

图 7-42:新建 IP 范围界面

地址组

地址组为 IP 掩码和 IP 范围对象的集合。

ue.			
项用地址		包括地址:	
	-2		
	2-		
1			

图 7-43:新建地址组界面



令 服务

设置服务识别防火墙接收或拒绝的通信会话类型。用户可以在策略中添加任何 预先定义的服务。用户也可以创建用户服务或在服务组中添加服务。

● 预定义

下图为查看预定义的服务列表。Anysec 系统设置的预定义服务目前有二十余种,基本上包含了用户使用率比较高的服务对象。

1	建文	自定文 服务组	
10	名称	详情	引用数
1.1	NC .	Cep/5900	0
2	ute	sulp/1-605.75	0
21	HIN.	trp/1389	0
٤.	#05321.	110/1433-1434	0
5	858	t-m/1663	0 1
6	IDAP	tap/388	ő
7	IICP	ndp/07-68	.0
×.	3/7	sep/178	0
9	BADING	tep/1812-1813	.0
10	STREET OF	u4p/514	0
11	TOP	±10/1-60526	0
12	MTSRL	\$xp/3306	0
13:	TFIP	mdp/65	0
11	PTHG .	A page / B.	0
10	APPERT.	A 44 / 18	

图 7-44: 预定义服务列表界面



● 自定义

当您的应用服务在自定义服务列表中找到时,您就需要在自定义服务对象功 能中新建了,以下为新建自定义服务的界面:

预定义	自定	※ 服务组			
		Ĩ	所建自定义服务		
服务名:]		
		目的	端口	调	「読」
协议	×	起始	结束	起始	结束
◎ TCP	o vop			1	65535
状态:	7				
		确;	定 取消	á	

图 7-45: 新建自定义服务界面

● 服务组

服务组为预定义服务和自定义服务的集合。

1名			
町東藤寺		后法解告	
VM WP NP X5TQL	1 🛛		
LDAP DHCP BGP	*		
1777. Ref. 101			



图 7-46: 新建服务组界面

◆ 时间

设置时间表控制激活与中止策略的时间。用户可以设置固定时间表或循环时间表。 使用固定时间表创建一项 策略在指定的时间段内生效。循环时间表每周进行一个循环。用户可以使用循环时间表设置一项策略只在指定的一天中循环几次或一 星期中某些天之内生效。

● 一次性时间

下图为新建一次性时间的操作界面

次性时间		循开时	IA .							
				新建	一次性利	調				
-8.83										
	单件	1	月	19	E	R.B.	de	时	24	14
开始	2010		01		01		.00		00	
停止	2010		01		01		00		00	
10.50	12									
		定					HX.	用		
		12.42	开始的	词成大	1000012	北京	保计时间			
		12.74	14 200-2	PLM AT	Windnak	#46-37-3.	SMIT diale			

图 7-47: 新建一次性时间界面

● 循环时间

下图为新建循环时间的操作界面



			新建设	研制詞			
名称	1						
EIM	重明日	堂明一	里圳二	里燈三	星期四	里明五	里路六
选择	19	1	(92)	100	12		2
开始	4	封	00 -	4	100	00 •	
停止	্য	81	00 ¥	4	神	• 00	
11:5:	12						
	- 10	定			Ex	周	
释 着你	止时间早于	井鹼时间.	财保止时间	是在第二天。	若开始时间	祷于维证时	间。适行时

图 7-48: 新建循环时间界面

◇ 地址转换

● 虚拟 IP(目的地址转换)

使用虚拟 IP 能够访问源网络中被 NAT (network adress translation: 网络 地址转换)安全策略隐藏的目标网络的 IP 地址。例如,您可以在外部网络 Anysec 设备接口添加一个虚拟 IP 地址,那么外部接口 就可以对实际上与 DMZ 或内部网 络中服务器连接的用户发出的请求作出回应。

下图为新建虚拟 IP 服务的操作界面。

失型 外部17类型	 ○ 网络地址转換 ○ 調応IF ● 職本IF
外部即地址	
外部编口范围	-
映射IF地址	
映射编口范围	
勘察	👁 TCP 💿 UDP

图 7-49: 预定义服务列表界面



● 源地址转换

下图为新建源地址转换的操作界面。

	新建築物材料系
	30 AL 10-10 AL 11 SH
源IP/Mank	192, 168, 0, 69 y 255, 255, 255, 255
目的17/Mask	202.111.21.23 / 255.255.255
流出推口	E3 •
协议	. IF O TCF O UDF
铸换后簿IP	202, 111, 21, 1
	勇定 取消
	機定 取 肩
	廣定 取 肩

图 7-50: 新建源地址转换设置界面

◇ IP/MAC 绑定

● IP/MAC 地址绑定设置

对于不在静态 IP/MAC 表中的内网 PC 数据做如何处理,处理方式包括:

允许: 仅允许不在静态 IP/MAC 表中的 PC 机发送数据包,静态 IP/MAC 表中的 PC 机发送的数据包将被网关设备拒绝;

拒绝: 仅允许在静态 IP/MAC 表中的 PC 机发送数据包,不在静态 IP/MAC 表中的 PC 机发送的数据包将被网关设备拒绝。

IP/MAC绑定投到	静态IP/MAC表	
	IP/MAC绑定设置	
对于7 系统书 ④ 5	《在静态IP/MAC表中的主机发送的数据包, 9采取的默认处理方式: 允许	
© 1	巨绝	
60	定	



● 静态 IP/MAC 表

对内网 PC 机进行 IP 地址和网卡 MAC 地址绑定,点击右上角"新建"即可添加。

IP/MAC纬	定设置 1	●杰IP/MAC表		100
当前IP/MAC	绑定数目: 0			L
ID	IP地址		MAC地址	编辑



♥ VPN 管理

Anysec 设备提供了多种 VPN 技术服务,在提供标准的 PPTP/IPSEC VPN 服务的同时, 也提供了个性化的,针对企业应用的点点通智能 VPN;针对移动办公应用的 SSL VPN 和 移动客户端服务。

◆ 点点通

点点通是 Anysec 设备针对企业用户推出的个性化的智能 VPN 解决方案。主要 分为两个部分。

- ✓ 设备隧道管理(终端支持)
- ✓ 隧道连接管理(平台支持)
- ◇ 设备隧道管理

● 配置

如何配置一个隧道: 点击 VPN 管理->点点通->配置菜单,可以看到下面的图示。

配置 隧道监控	设备管理	连接管理	在线设备
	뀭	备配置	
设备名	devid	ce3	
设备ID	1002		
通讯密码	••••	••	
隧道策略	寻址方式:		
) 通过	过公网IP或域名寻址		
() 通过	dSecROS网络平台寻址	t	
策略中心:	地址 myspa	ace	
上级策略	中心地址		
现在激活			
	确	定	



图 7-51: VPN 管理下设备配置界面

设备名、设备 ID、通讯密码是在隧道连接管理定义的,设备名和设备 ID 用 于表示一个拥有点点通隧道的 Anysec 设备身份,通讯密码是 Anysec 设备到隧道 连接管理平台的认证密码。

策略中心地址是隧道连接管理平台的地址,可以是 IP 地址,也可以是一个域 名。

现在激活表示点点通隧道的状态是否生效。

● 隧道监控

如何监控隧道状态:

点击 VPN 管理->点点通->隧道监控菜单,可以查看点点通隧道的状态。

下图为点点通隧道的监控界面。您可以点击"测试"按钮测试当前隧道是否 正常连通。

图 7-52: VPN 管理下隧道监控界面

● 隧道连接管理

隧道连接管理是点点通平台的一个重要功能,用于定义点点通设备和隧道策 略。

● 设备管理

如何定义一个点点通设备:

点击 VPN 管理->点点通->设备管理页面里面的新建按钮,可以新建一个点点 通设备对象。

下图为新建设备的界面。



配置	隧道监控	设备管理	连接管理	在线设备	
		新	建设备		
	设备名	研发中心			
	设备ID	1003			
	通讯密码	•••••			
	联网模式	动态公网	IP或NAT设备后 🔻	·	
	内网口IP	192.168.	0.99		
	在线生存期	300	(120-3600	秒)	
	联系人	王盼			
	电话	13713867	534		
	备注	研发中心			
	确定	取	消		

图 7-53: VPN 管理下新建设备配置界面

设备名与设备 ID 表示一个点点通设备的身份,其中设备 ID 和设备名都必须 唯一。

通讯密码用于设备到平台的身份认证。

联网模式表明该设备的上网方式。

内网 IP 是设备的内网口 IP 地址,也是用于建立隧道的内网地址。

下图为设备列表界面。



r 市			古林生						
马 设备名 设备10 内间口1P — 種孢子树 和何万式 (NP) 看注	-1842	指注	存期 (秒)	顺列方式	羅道子阿	内间口口	设备11	设备名	席马
1 課发中心 1003 102 168 0.99 和工资量后 300 被发中心	n 26	時日本	- 200	动态公园印度		100 100 0 000	1000		

图 7-54: VPN 管理下设备列表界面

新建设备成功后,您还需要对该设备的隧道子网进行定义,请点击"隧道子 网定义"图标,按照实际情况将隧道子网一一加入即可。

下图为隧道子网定义界面:

RE	局消益技	10 25 59 M	正接管理	有线营养
	2回之	新建制及	PHOTOCOMPRESS PHOTOCOM	
	TEND		192, 168, 32, 0	
	网络捕猎	8	255, 255, 255, 0	
	17793	-	1552 2151 35 PA	
		構定	取消	

图 7-55: VPN 管理下设备隧道子网配置界面

● 连接管理

如何定义一条隧道策略:

点击 VPN 管理->点点通->连接管理菜单,选择一个设备,点击"修改连接策略"按钮,将出现下图所示的界面。



		编辑连续	ESE HE		
計名	「観光中心」				
可互联设	*	2	已违设备 营销中心	2 2	
		100 100	HY MI		

图 7-56: VPN 管理下新建连接策略设置界面

从可互联设备列表中选择需要建立隧道的设备到已选设备列表即可。 当需要互联的两台设备都处于 NAT 环境中如何处理:

点击 VPN 管理->点点通->连接管理菜单,选择其中一台设备,点击"修改连 接属性"按钮,在出现的连接列表中选择"修改连接属性"按钮,将连接方式由 "直接连接"改为"第三方中转",并选择相应的中转设备即可。

● 在线设备

如何查看点点通隧道与设备状态:

点击 VPN 管理->点点通->在线设备菜单,可以查看在平台内定义的所有设备的在线状态和隧道状态。



下图为在线设备界面。

- NC	2 R3	國設設	设备管理	18	林官權	在信息系		
19	检察者	1441B	NET	HAT JS	EXH	在城生存期 (秋)	当前 状态	靈作
1	derine)	1602	219, 133, 58, 40	H	Fri Jan 22 00. 27. 10 2010	999		Q. 陶砂袋 (2
=	北田水事社	1005	114.117.14.45	H	Fri Jan 82 09 35:25 2010	300		0.842

图 7-57: VPN 管理下在线设备显示界面

您可以点击"设备详情"按钮查看当前设备的基本情况,例如设备名、设备 ID、设备型号及类型、软硬件版本,认证 IP 地址以及 WAN 链路情况。

投資格	devises?
设备加	
设备型号	3601.0.0
设备类型	230
软件版本	20100120-2009 vint.
硬件质本	borbutur-mee
ikiErr	219, 113, 88, 49
取阿提式	助高公园IF #INAT 设备后 -

图 7-58: VPN 管理下在线设备详情界面

您也可以点击"隧道状态"查看与该设备互联的所有隧道情况。



arte l	联邦当时 首音管理	は単世世 遺猿方式	中转设备名	展示状态
1	day and the month and	肉体古物		10

图 7-59: VPN 管理下在线设备隧道状态界面

您还可以点击"在线设备控制"按钮,对设备进行简单控制:

· 這發媒的 ● 市存当用运行政医 ● 所有"当用运用			
一 地田市福岡造場			
广始联网 ● 曲道/1989			
○ 集發於新述指導的			
● 重建的有能量	● 重建的有能量		
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	● 排件出稿提出版		
中国報告			
防火橋 ○ 美記納发			

图 7-60: VPN 管理下在线设备控制设置界面



♦ PPTP

Anysec 设备支持点对点通道协议进行两个对等体之间的 PPP 通讯流量。 Windows 或 Linux PPTP 用户可以与配置作为 PPTP 服务器的 Anysec 设备建立一个 PPTP 通道。用户 也可以配置 Anysec 设置将 PPTP 数据包转送到置于 Anysec 设备之后的网络中的 PPTP 服 务器。 PPTP 配置只适用于 NAT/路由模式。当前 PPTP 与 L2TP 会话的最大数量为 254。 起始与结束的 IP 必须在相同的 24bit 的子网中,例如 x.x.x.1-x.x.x.254。

● 参数配置

如何设置 PPTP 服务:

点击 VPN 管理->PPTP->参数配置菜单,可以配置 PPTP 服务,如下图所示。

5002	在线用户	
		FFTF设置
	起始IF地址:	192, 168, 99, 1
	最大接入数:	200
	认证用户组:	WebAuth -
	服务状态:	
		确 定

图 7-61: PPTP 设置界面

起始 IP 地址和最大接入数定义了 PPTP 接入后分配的 IP 范围和 PPTP 服务的 最大连接数目。

认证用户组可以选择 PPTPAuth 认证用户组,也可以选择其他用户组。 服务状态表明 PPTP 服务是否开启。

在线用户

显示当前通过 PPTP 方式接入网络的在线用户情况。

	田白幺	当前开始研	職者建立时间	緩白
-	101.000	COLUMN AN ACCOUNT	and the stand here	38.1
	And the state	Sector Contractor	100 C C C C C C C C C C C C C C C C C C	

图 7-62: PPTP 在线用户显示界面



♦ IPSEC

Anysec 设备支持 IPSEC VPN,提供了标准的 IKE/IPSEC 服务,能够与第三方设备互联,同时还提供了手工指定 SPI 方式建立 IPSEC 隧道的快速服务和隧道查看功能。

关于 IPSEC 接口模式:

在用户定义 IPSEC 隧道的时候,需要将设备的 IPSEC 接口绑定到内网口上,默认出 厂配置里面 IPSEC 接口的 IP 是 127.0.0.1。

● 手动模式

手动模式是 Anysec 设备提供的一种快速建立 IPSEC 隧道的特殊功能,省去了 IKE 协商,直接输入 IPSEC 隧道建立的所需参数。

		BI ME - 7 - 40 DE 15		
隨港名	test			
本地SPI	201	(HEX)		
远端SPI	202	OBX		
远端网关	119, 123, 8, 10			
加密算法	3DES 👻			
加密密制	•••••	•••		••••
		••		
认证解选	MD5 -			
加密密铜		••	•••••	••••
IPSEC模式	@ 接口模式 ()	第編儀式		
本地子网	192. 168. 0. 0/24			
远端子网	192.168.119.0/24	1 m		

下图为添加一条手动隧道的操作界面。

图 7-63: 新建手动模式隧道配置界面



● 如何与第三方设备建立 IPSEC VPN

Anysec 设备支持与第三方 VPN 设备建立 IPSEC VPN。需要建立 IPSEC VPN 的 双方设备采用 IKE 密钥交换协议进行身份认证和密钥协商, IKE 协议分为 2 个阶段。

● IKE-阶段 1

下图为新建 IKE-阶段 1 的操作界面。

手动模式	IKE-阶段	1 IKE-阶段2	IKE模式	隧道监视器	
		新建IKE-阶段1			
	阶段1名称	home			
	远程网关类型	静态IP	•		
	IP地址	123. 23. 112. 21			
	模式	💿 主模式 👘 💿 野蛮模式	t		
	认证方式	预共享密钥	•		
	预共享密钥	•••••			
	高级选项	(Nat Traversal, XAUTH, D	PD)		
	竹注担议。「	2			
	中本征以 []	3DES CBC -	1		
	山证算法 1	MD5 -]		
		WODP1024 -			
	ладид Т	•]		
	密钥生存期 2	28800	(120-86400	秒)	
	⊼扩端ID γ	vangpan@anysec.com		(可选)	
	本端ID	jeftluo@anysec.com		(可选)	
	NAT-T支持 [V			
	YAIITH (
	ANOIN (♥ 小启用	◎ 服労番勁	ή 	
	DPD支持 [V			



图 7-64: 新建手动模式隧道阶段 1 配置界面

▶ 阶段一名称

用户在新建一个 IKE-阶段 1 配置的时候,需要为这个配置起一个名称,该名 称必须在阶段 1 的所有配置中是唯一的。

➢ 远程网关类型

远程网关类型是描述对端设备的上网方式,可以是静态 IP 或者域名(也包括 动态域名)。

▶ 模式

IKE 第一阶段协商支持 2 种模式,一种是主模式,一种是野蛮模式,请与需要建立隧道的设备保持相同模式。

▶ 认证方式

认证方式分为预共享密钥和证书认证两种方式,如果采用预共享密钥方式, 则需要填入事先约定的密码,如果采用证书认证,则需选定本地设备证书和对端 设备证书,证书在系统管理->证书功能里面配置。

▶ 算法

用户可以在 IKE 阶段一协商中选定需要使用的加密算法和认证算法。

➢ 密钥生存期

密钥生存期是指 IKE 阶段一协商出来的密钥的有效期,请与需要建立隧道的 设备保持相同的密钥生存期。

> ID

ID 是表示本端和对端设备身份的一个标识,如果采用证书认证模式,则 ID 不需要另外填写,采用预共享密钥方式建立隧道,必须保证需要建立隧道的两个

69



设备的 ID 一致。

▶ NAT-T 支持

NAT-T 支持是用于穿越 NAT 设备的功能。

> XAUTH

XAUTH 认证是扩展认证,分为客户端和服务器端,提供用户名/口令模式认证。

➢ DPD 支持

DPD 支持是心跳检测功能。

• IKE-阶段 2

下图为新建 IKE-阶段 2 的示例界面。

手动模式	IKE-B	介段1	IKE-阶	段2	IKE模式	隧道监视器
			新建IKE-防)段 2		
阶段	阶段2名称		officelan			
本辨	本端网络地址		192.168.0.0/255.255.25		55.0	
对韩	腳络地址	192.16	8.1.0/255.	255.28	55.0	
高級	及选项					
 算〉	法提议	V				
500 July	密算法	3DES		•		
પ્રાં	正算法	MD5		•		
密約	钥生存期	28800			(120-86400 秒)	
	确定		EX 3	肖		

图 7-65: 新建手动模式隧道阶段 2 配置界面

▶ 阶段2名称

用户在新建一个 IKE-阶段 2 配置的时候,需要为这个配置起一个名称,该名称必须在阶段 2 的所有配置中是唯一的。



> 本端网络地址

用于指定 VPN 隧道的本端网络信息。

> 对端网络地址

用于指定 VPN 隧道的对端网络信息。

▶ 算法

用于指定 IPSEC 隧道的加密算法和认证算法。

> 密钥生存期

用于指定 IPSEC 隧道的密钥的有效期,请与需要建立隧道的设备保持相同的 密钥生存期。

● IKE 模式

IKE 模式功能是在 IKE-阶段 1 和阶段 2 的基础上,创建 IPSEC VPN。如果设备 处于防火墙后面或需要主动发起连接,则选中主动连接按钮。

下图为新建 IKE 模式隧道的示例界面。

手动模式	IKE-阶段1	IKE-阶段2	IKE模式	隧道监视器
隧道	道名 work	vpn		
IKE	-阶段1 home	9	•	
IKE	-阶段2 rdla	an-officelan	•	
主革	加连接 🔍			
_	确定	取消		

图 7-66: 新建 IKE 模式隧道配置界面

● 隧道监视器

Anysec 设备提供 IPSEC VPN 隧道查看功能,可以查看手动隧道和 IKE 隧道。 下图为隧道监视器界面。





图 7-67: 隧道监视器界面

\diamond SSL VPN

Anysec 设备提供 Web 转发保护的 SSL VPN 功能。

● 参数配置

下图为 SSL VPN 设置的操作界面。

参数配置	SSL隧道			
		SS	SLVPN设置	
服	服务器证书:		-	
验	验证客户端证书:			
客	户端超时:		10	
服	务器超时:		15	
服	服务状态:			
			确定	

图 7-68: SSLVPN 设置界面


服务器证书是 Anysec SSL VPN 的设备证书,在系统管理的证书功能中加载或 产生。

验证客户端证书是 SSL 的一项安全措施,可以要求设备验证客户端证书,确 保用户身份。

客户端超时和服务器超时是用于维护 TCP 会话的时间参数,通常采用默认值。 服务状态表示是否开启 SSL VPN 服务。

• 创建 SSL 隧道

下图为新建 SSL 隧道的操作界面。

参数规语	医虹膜炎			
		新建SSL题	0	
	随着名 IF地址 端口			
	用户组: 描述	WebAuth	•	
	机定	取 開		

图 7-69:新建 SSL 隧道配置界面

隧道名是 SSL VPN 的名称,必须保证唯一。 IP 地址是 SSL VPN 后台的 WEB 服务器的 IP 地址。 端口是 SSL VPN 后台的 WEB 服务器的端口。 用户组是用于指定身份认证的用户集合。 描述是用于表述该条 SSL VPN 的用途。



◆ 移动客户端

Anysec 设备的移动客户端是 Anysec 针对移动客户的接入需求,在 IPSEC VPN 技术的基础上优化推出的一个 IPSEC 隧道客户端功能,支持用户名/口令认证和证书认证。

移动客户端软件分为服务器端和客户端两大部分,其中服务器端的配置在 Anysec 设备上通过 WEB 或 CLI 来操作;客户端是一个运行在 Windows 系统下的 应用程序,用户在使用前必须先运行移动客户端安装程序。

● 配置服务端

下图为移动客户端接入配置界面。



配置	隧道子网	在线用户	
		移动客户	端接入设置
	起始IP地址:	1	0. 0. 0. 2
	结束IP地址:	t	0. 0. 0. 100
	支持PKI认证:	[
	认证用户组:	1	ClientAuth 👻
	服务状态:	[7
			确定

图 7-70: 移动客户端接入设置界面

起始 IP 地址和结束 IP 地址用于定义分配给移动接入的用户的 IP 地址范围。 支持 PKI 认证是开启证书认证功能。

认证用户组是定义验证移动接入用户的身份识别的用户组。 服务状态是表明是否开启接入功能。

● 定义隧道子网

配置移动客户接入设置后,必须定义隧道子网,将 Anysec 设备非 WAN 接口的网段中,需要提供给移动客户访问的网段添加到隧道子网中,否则移动客户接入后还是无法访问内部网络。

下图为隧道子网的列表示例图。



图 7-71: 移动客户端隧道子网列表界面

下图为新建隧道子网示例图。



122	間到子间	在线用户 新建能過子网	
	子网名 12地址 子网境码		
	状态: 		

图 7-72: 新建移动客户端隧道子网界面

● 在线用户

显示当前通过移动客户端接入的用户列表。通过该界面我们可以非常清楚的 知道当前有哪些用户已经通过移动客户端软件或 Key 接入进来,用户的 IP 地址以 及隧道建立的时间等信息。

隧道子	网 在线用户		
用户名	当前IP地址	隧道建立时间	编辑
王盼	10.0.0.2	Fri Jan 22 09:50:15 2010	
	隧道子 用户名 王盼	隧道子网 在线用户 用户名 当前IT地址 王盼 10.0.0.2	隧道子网 在线用户 用户名 当前印地址 隧道建立时间 王盼 10.0.0.2 Fri Jan 22 09:50:15 2010

图 7-73: 移动客户端在线用户显示界面

◆ 配置客户端

1、安装客户端后,运行移动客户端程序会出现如下图所示的程序。



	ANYSEL	10
ANYSE	C 83	客户端 V6.0
演进探要注接的道道	8	•
连接	10 2	8.8

图 7-74: 移动客户端界面

2、点击"设置"按钮,出现高级设置窗口,可以查看已经建立的隧道,也 可以建立新的隧道。

0501249 			
1 建油合称	-		Ð
a tu	ei ta	修改	 87
強調注紙信用			 -
			 _

图 7-75: 移动客户端高级设置界面

3、点击"添加"按钮后,出现隧道配置框。



隧道	隧道名称	中科网威总部
	寻址方式	SecROS简域 👤
	SecROS简掝	anysec
隧道	设备名称	总部
	用户名	王盼
	口令	*****
	□ 保存口令	
	□ 使用文件	证书验证 证书设置
	☐ 使用SecR	OS VKey认证
	确	定 取消 之

图 7-76: 移动客户端隧道配置界面



使用证书验证:

→该设置勾选后能保存用户名和密码。

→如果使用证书认证方式请勾选使用证书。



CONTRACTOR AND A REAL PROPERTY OF A DESCRIPTION OF A DESC		*
系統高級设置性 「是否支持的线量 新线重新间隔(秒) 「一并机自动履道 - 虚拟网末设置性 	(南科阿威 (((((((((((((((((((
Ŭ	定	取清

4、在高级设置窗口点击高级可以配置系统设置框,如下图所示。

图 7-77: 移动客户端系统设置界面

系统设置框提供了断线重联和开机启动功能。

另外,还提供了虚拟网卡的管理功能,用户如果发现虚拟网卡出现问题,可 以卸载或安装新的虚拟网卡。



⊃ 行为管理

Anysec 行为管理是与防火墙功能相结合,向用户提供上网行为管理功能,用户在行 为管理模块里面定义各种上网行为管理策略,必须在防火墙策略里面引用这些行为策略 才能让设备进行上网行为管理。

上网管理策略包括了:

➢ DNS 策略

> 网页策略

> 文件策略

> 邮件策略

DNS 策略可以提供 DNS 屏蔽和 DNS 免屏蔽, 通过 DNS 来控制用户对特定网站的访问 控制。

网页策略是 URL 级的访问控制, 粒度更细。

文件策略是使用文件后缀名作为控制条件的访问策略。

邮件审计 Anysec 针对邮件管理提供的一项高级功能,可以对邮件发送进行审计,可 以制定免审计邮件和审计配置。

◇ 定义行为管理策略

点击行为管理->行为规则菜单,可以配置上网行为管理策略。

注意:您的行为管理策略需要在防火墙的访问控制中引用才能生效。

- 19 SAN CIMA U.S. SAN 1 Springer 1 2
- 查看行为定义

ID: 行为的序号。

名称: 行为名称, 被防火墙策略采用。

图 7-98: 行为定义列表界面



引用数:行为被引用的次数。 **状态**:行为是否被激活的状态。

新建行为定义

	新潮行力推拔	
NIS IS	E.	
DNS80### DNSM##	- hen - •	
, HEIDM		
い有金銀石	- New - +	
URLINI	The Trace + +	
Websertheast	E	
ActiveXidtill	8	
Java Appletztitt	23	
Www.economia	E	
, XNIDM		
Rective.	- hop - +	

	唐和白彩													
	QQ MSP	2	同糖莊 杜	RMB B	-	Thips	Web	99						
明止		17	10	0	10	.0	0							
	BRACK													
mr.	QQmit El	000 13	MR2 =		PQ:: 1	8次約43 日	RM () (PREMIER	HUE GOM	Distance in the second se	236293	t)		
	LERICH													
0.00	信存之間	大教領	利花離	常樹肉	阿上南市	F 168.5	納納	MARCHEN	化大运用	「秋田田	前的正形	把考证存	联合证券	国内沿井
和此	12	01	E	1		12.1	0	-63	1	E3.	11	10	13	61
P2P	RINISH													
RE	PPSIzier	PPIn 10	* QQI	ve 52,0	QVOD	UU5ee	11.64							
• P2P	TRIEM													
14-121				BTTH.		1634	è	. 10	3.8		PRRIE		包裹下吧	
1645				Pum		- Par			Fars . +		Pore .		Para 🔹	
1643	BESITE IN	60.0							1		1			
							R		a a					

图 7-99: 新建行为属性设置界面

名称:指定新建行为的名称,用于防火墙策略里面的上网行为策略。 **态**:表明新建行为是否激活有效。 状

DNS 控制:包含了 DNS 行为控制,可以选择 DNS 定义里面的各种策略。

网页控制:包含了网页行为控制,可以选择网页定义里面的各种策略,可以控制 Web 邮件发送过滤, ActiveX 过滤和 Java Applet 过滤、Web 视频屏蔽。

文件控制:包含了文件行为控制,可以选择文件定义里面的各种策略。

邮件控制:可以启用发件审计功能。

IM 控制、在线游戏、证券控制、P2P 视频控制、P2P 下载控制:可以控制 QQ、MSN、



飞信、阿里旺旺、网易泡泡、雅虎通、Skype、WebQQ、QQ 游戏、联众游戏、中国 游戏中心、浩方对战平台、网易泡泡游戏、边锋网络游戏、农场游戏、证券之星、 大智慧、同花顺、龙卷风、网上赢家、钱龙、分析家、麒麟短线王、光大证券、广 发证券、国信证券、招商证券、联合证券、国元证券、PPStream、PPlive、QQlive、 快播 QVOD、UUSee、沸点电视、BT 下载、电驴、迅雷、超级旋风、百度下吧等常 见应用行为。

♦ DNS 定义

DNS 定义包括 DNS 屏蔽和 DNS 免屏蔽功能。

● DNS 屏蔽

如何进行 DNS 屏蔽:

点击行为管理->DNS 定义->DNS 屏蔽, 点击右上角的"新建"图标, 输入 DNS 屏蔽组名, 例如 ppstream, 点击"确定"按钮。通过以上步骤, 您已经新建了一个名为"ppstream"的 DNS 屏蔽组, 如下图:

DNS	F蔽 DNS免	屏蔽			
ID	组名	域名数目	引用数	状态	编辑
1	ppstream	0	0	V	📸 📝

图 7-78: DNS 屏蔽列表界面

接下来,您可以点击编辑栏中的"修改"图标,对 ppstream 组中的 DNS 进行定义。



	DNS 屏蔽 DNS 免 屏蔽				
		编辑域名屏	蔽组		
	组 名 ^{ppstre}	am	☑ 确 定		
ID	域名/表达式	匹配类型	匹配数	状态	编辑
1	fds.pps24.com	通配符	0	1	📸 🌛
2	*, pps. tv	通配符	0	1	🗃 🌛
3	*.ppstream.com	通配符	0	1	📸 🌛

图 7-79:编辑域名屏蔽组界面

请点击右上角的"新建"图标,并在输入框中输入您希望屏蔽的 DNS。如下图:

DNS屏蔽	DNS免屏蔽		
		新建域名屏蔽成员	
ł	域名/表达式	www.abcd.com	
[匹配类型	通配符 👻	
*	伏态		
	确定	取消	

图 7-80: 新建域名屏蔽成员界面

例如我们输入"www.abcd.com",依照此方式,您可以逐个加入您想要屏蔽的 DNS。

● DNS 免屏蔽

如何进行 DNS 免屏蔽:

DNS 免屏蔽功能是相当于 DNS 屏蔽功能而言的。例如您在 DNS 屏蔽中设置 了屏蔽 "*.abcd.com",但你又不想屏蔽 "news.abcd.com",那么该如何设置呢?

首先我们按照 DNS 屏蔽的设置步骤将"*.abcd.com"加入到 DNS 屏蔽组中, 接着我们依旧按照和 DNS 屏蔽类似的步骤来处理"new.abcd.com"这个免屏蔽域 名,具体步骤如下:

点击行为管理->DNS 定义->DNS 免屏蔽,点击右上角的"新建"图标,输入 DNS 免屏蔽组名,例如 DNSEXEMPT1,点击"确定"按钮。通过以上步骤,您已 经新建了一个名为"DNSEXEMPT1"的 DNS 免屏蔽组,如下图:

DNS	お話 DNS免損	祥蔽			
ID	组名	域名数目	引用数	状态	编辑
1	DNSEXEMPT1	0	0	V	🗃 🌛

图 7-81: DNS 免屏蔽列表界面

接下来,您可以点击编辑栏中的"修改"图标,对 DNSEXEMPT1 组中的 DNS 进行定义。

DN	S屏蔽	DNS免屏蔽				
	编辑域名屏蔽组					
		组 DNSEXEM	PT1	☑ 确	定	
		-				
ID	域名	/表达式	匹配类型	匹配数	状态	编辑

图 7-82:编辑域名屏蔽组界面

请点击右上角的"新建"图标,并在输入框中输入您希望免屏蔽的 DNS。如 下图:



DNS屏蔽	DNS免屏蔽	
		新建域名免屏蔽成员
	域名/表达式	news. abcd. com
	匹配类型	通配符 🚽
	状态	
	确定	取消

图 7-83: 新建域名免屏蔽成员界面

例如我们输入"news.abcd.com",依照此方式,您可以逐个加入您想要免屏蔽的 DNS。

◇ 网页定义

网页定义包括 URL 屏蔽和 URL 免屏蔽。

● URL 屏蔽

如何进行 URL 屏蔽:

点击行为管理->URL 定义->URL 屏蔽, 点击右上角的"新建"图标, 输入 URL 屏蔽组名, 例如 URLBLOCK1, 点击"确定"按钮。通过以上步骤, 您已经新建了 一个名为"URLBLOCK1"的 URL 屏蔽组, 如下图:

URL	Taka URL免疫	祥蔽			
ID	组名	URL数目	引用数	状态	编辑
1	URLBLOCK1	0	0	V	📸 🌛
2	tieba	8	1		📸 🌛

图 7-84: URL 屏蔽列表界面



接下来,您可以点击编辑栏中的"修改"图标,对 URLBLOCK1 组中的 URL 进行定义。



图 7-85:编辑 URL 屏蔽组界面

请点击右上角的"新建"图标,并在输入框中输入您希望屏蔽的 URL。如下图:

URL屏蔽	URL免屏蔽		
		新建URL屏蔽成员	
ι	RL.	http://lady.163.com/*	
7	方式	GET 👻	
1	犬态	\checkmark	
1	确定	取消	

图 7-86:编辑 URL 屏蔽成员界面

例如我们输入"http://lady.163.com/*",依照此方式,您可以逐个加入您想要屏蔽的 URL。

● URL 免屏蔽

URL 免屏蔽功能是相当于 URL 屏蔽功能而言的。例如您在 URL 屏蔽中设置了 屏蔽 "http://lady.163.com/*",但你又不想屏蔽 "http://lady.163.com/special/*", 那么该如何设置呢?

首先我们按照 URL 屏蔽的设置步骤将 "http://lady.163.com/*" 加入到 URL 屏蔽 组中, 接着我们依旧按照和 URL 屏蔽类似的步骤来处理



"http://lady.163.com/special/*"这个免屏蔽 URL,具体步骤如下:

点击行为管理->URL 定义->URL 免屏蔽,点击右上角的"新建"图标,输入 URL 免屏蔽组名,例如 URLEXEMPT1,点击"确定"按钮。通过以上步骤,您已 经新建了一个名为"URLEXEMPT1"的 URL 免屏蔽组,如下图:

URL.	お話 URL免疫	祥蔽			
ID	组名	URL数目	引用数	状态	编辑
1	URLEXEMPT1	0	0	V	📸 🌶

图 7-87: URL 免屏蔽列表界面

接下来,您可以点击编辑栏中的"修改"图标,对 URLEXEMPT1 组中的 URL 进行定义。

URL 屏蔽	URL免屏 調	ŧ				
	编辑URL免屏蔽组					
	组 化RLEX	EMPT1	☑ 确 定			
ID	URL.	方式	匹配数	状态	编辑	

图 7-88:编辑 URL 免屏蔽组界面

请点击右上角的"新建"图标,并在输入框中输入您希望免屏蔽的 URL。如下图:

URL屏蔽	URL免屏蔽	
		新建URL免屏蔽成员
1	/RL	http://lady.163.com/special /*
5	方式	GET 👻
1	犬态	
	确定	取消

图 7-89:新建 URL 免屏蔽成员界面

例如我们输入"http://lady.163.com/special /*",依照此方式,您可以逐个加 入您想要免屏蔽的 URL。



◆ 文件定义

文件定义包括文件类型屏蔽,其依据文件的后缀名对文件进行过滤。目前支持的能够对文件后缀名进行过滤的协议有四种:HTTP、FTP、SMTP和 POP3。

● 文件类型屏蔽

如何进行文件类型屏蔽

点击行为管理->文件定义->文件类型屏蔽,点击右上角的"新建"图标,输入文件类型屏蔽组名,例如 FILEBLOCK1,点击"确定"按钮。通过以上步骤,您已经新建了一个名为"FILEBLOCK1"的文件屏蔽组,如下图:

文件	类型屏蔽				
ID	组名	文件数	引用数	状态	编辑
1	FILEBLOCKI	0	0		🗃 🌛
1	FILEBLOCKI	0	0	V	1

图 7-90: 文件类型屏蔽列表界面

接下来,您可以点击编辑栏中的"修改"图标,对 FILEBLOCK1 组中的文件类型进行定义。

文件	类型屏蔽					
编辑文件类型屏蔽组						
	组 名	FILEBLOCK1		☑ 确	定	
ID	文件类型	HTTP	FTP	SMTP	POP3	编辑

图 7-91:编辑文件类型屏蔽组界面

请点击右上角的"新建"图标,并在输入框中输入您希望屏蔽的文件类型。 如下图:



文件类型屏蔽					
文件类型 *. exe 如 *. exe 如 *. exe					
HTTP					
FTP	\checkmark				
SMTP	\checkmark				
POP3	\checkmark				
确定	取消				

图 7-92: 新建文件类型屏蔽成员界面

例如我们输入"*.exe",然后选择相关协议,依照此方式,您可以逐个加入 您想要屏蔽的文件类型。

◆ 邮件审计

Anysec 设备具备邮件延迟审计功能,当内网用户使用邮件客户端通过 SMTP 协议发送邮件时,如果防火墙策略匹配到该用户所发送的邮件需要进行延迟审计 后才能发送,那么该用户所发送的邮件将被 Anysec 临时收藏起来,待邮件审核 员对该邮件进行审计通过后,该邮件才能发送出去。而这一切对于刚才发送邮件 的用户来说是完全透明的。当有邮件需要审计时,Anysec 系统会依据审计配置向 审计员发送一封提示邮件,以告知审计员及时处理邮件以免耽误他人工作。

Anysec 邮件审计功能包含三个部分:

● 发件审计

用户发送的所有需要审计的邮件都会存放在发件审计列表中,一般情况下, 只有当审计通过后,该邮件才会发往 Internet。

8	发件人	東件人	主題	秋水 明朝			

图 7-93: 发件审计列表界面



● 免审计邮件

免审计邮件用于对一些特殊的邮件发送人或接收人进行免审计处理,发件人 或接收人必须至少输入一项。

名称	1		1	
发件人				
收件人				
状态	N.			
1.48	10 m			
		-	-	

图 7-94: 新建发件白名单界面

● 审计配置

申计负配置: 第11個称答:		
兼創件地址:		
車计员通输:		
1877服务器需要验证用户名和密码:	10	
登录用户名 (
那吗 :		
邮件审计策略:		
未审计审计版记时间超过:	60	分钟后, 该邮件将被自动 发送 *
制件发送失败最大密试次数:	3	*
叠创研 和 发送的件:	173	

图 7-95: 新建发件审计配置界面

- > SMTP 服务器: 指发送审计提示邮件使用的 SMTP 服务器地址。
- ▶ 源邮件地址:指发送审计提示邮件的源地址。
- ▶ **审计员邮箱:** 审计员接收提示审计邮件的 Email 地址

当 SMTP 服务器需要验证用户名和密码时,您可以勾上复选框,并输入登录 用户名和密码。



▶ 邮件审计策略:

当需要审计的邮件由于某种原因未能及时审计发送时,该审计邮件将会依照 邮件审计策略进行处理:自动发送或删除。

● 发件备份(高端设备具有)



图 7-96: 新建发件备份列表界面

将邮件备份在 ANYSEC 安全网关中。



◆ 带宽控制

Anysec 产品提供一种非常简易的带宽控制功能以处理由于 P2P 等软件造成带宽滥用 而影响正常的网络工作,您只需要简单的指定 IP 地址,并设置其最大带宽即可。注意: 该功能主要用于处理非正常情况造成的网络带宽滥用,该功能设置的 IP 带宽在设备重启 后将不再有效。如果您需要对网络带宽进行有效管理,您可以通过防火墙的策略来对带 宽进行定义。

下图为新建 IP 带宽管理界面。

UCENNE			
	#1	17带微管理	
12,169	ė	0.0.0.0	
最大	南魏 (Bps.)		
	有一百年	Second Co	

图 7-97: 新建 IP 带宽管理设置界面

Э 网络监控

网络监控功能是 Anysec 设备的特色功能之一, 您可以通过该功能了解内网用 户的上网情况。

支持哪些网络监控?

Anysec 设备支持以下网络监控功能:

◆ 定义监控规则

点击网络监控->监控规则菜单,可以配置网络监控策略。

注意:您的网络监控策略需要在防火墙的访问控制中引用才能生效。



● 查看监控规则



图 7-118: 流量规则列表

ID: 监控规则序号。

名称:监控规则名称,被防火墙策略采用。 **引用数:**监控规则被防火墙策略引用的次数。 **状态:**监控规则当前是否被激活的状态。

新建监控规则

-		8527987
6301		
881	(C)	
. HREN		
****	-	
A DALER		
INCOME.	(A)	
. PERMIT		
INL-OF TAXED		
Int-recent digit	10	
versitif.		
(TELED)		
10425	10	
******	12	
- SAR		
unigr		
LANCE N	12	
mager	-	
		Concession Concession

图 7-119: 新建监控规则界面

◆ 监控选项

Anysec 设备支持远程存储监控日志



监控定义	监控选项	
	监控计	先项设置
启用远程存储 远程存储服务	5器IP:	
	荷	自定

图 7-125:监控选项界面

若选择远程存储日志服务器,请先确认远程存储服务器进程是否已启动。

◇ 流量监控(具体功能依产品型号不同而不同)

Anysec 能对每个 IP 的网络流量进行记录和统计,并以图表的形式直观的展示 出来。Anysec 设备能显示实时带宽、5 分钟流量统计、小时流量统计、日流量统 计和月流量统计。

● 实时带宽:



图 7-100: 实时带宽列表

● 5 分钟流量统计表:

实时带宽	513141	- da	(注意图)	日金银	月读集			
11/瓶户	白田	发送总里	建收总型	TEPHIQ	加加协议	ICHP协议	mithiz	料它
192 168 118 100	9.51	2.38	7.50	1.19	1.18	0	7.28	0
田神	8.28	2.38	7 (18	1.28	2.18	u	7.78	61

图 7-101:5 分钟流量统计表



● 小时流量统计图:



图 7-102: 小时流量统计图

- 月流星 Last 1 Day Traffic 60 5555333555 1 1 Traffic (Muture 5 14.05 03154 04:54 10110 01154 Time(hour) IEMP 🛛 RTEP 🔤 ALL 109 100
- 日流量统计图:

图 7-103: 日流量统计图



● 月流量统计图:



图 7-104: 月流量统计图

♦ DNS 监控

Anysec 设备能监控并记录内网用户所有 DNS 请求情况:(型号不同表现形式 会有不同),中端型号一般只显示最新的 200 条 DNS 访问信息,一般高端型号能 够依据日期进行 DNS 访问记录,并能内网 IP 来查询其所以访问过的 DNS,同时 也可以通过 DNS 来查询哪些内网 IP 用户访问过该 DNS。

and the	automit 2 City		4
18	TP/III/P	ALFA	168
0	100 110 101 127	F() Jac 10 10 (1/0 000)	12. Staaling m
2	100 100 23 229	- 0101 101 00 101 00 40 101 0010	Lo senality as
1	100.166,59.117	1 Fei Jas 20:10 40. St 2010	adh aine ann an
4	100 100 300 127	Pys Jac 23:10, 41, 91, 3010	adh nine on m
51	10E 100 TH 117	701 Jan 12 50 40 71 2010	the strength on
6	100.100.000.107	Fil Jan 22 10 41 51 2010	evention not en-
¥	100 100 308 107	Fee 34 12 10 42 61 2410	ere dias not in
	DAE: 000 TH 117	first Jac and not do the manth	the allering an
1	102 108 20 127	Fri Jan 12 10 41 10 1010	ees aray not in
10	112 180 101 127	Prr 144 12 10 41 10 2110	eve stan me in
11	DE DOUTR ET	Here day not not the ser anno-	10 sinaing m
411	100.000.000.007	Feb Jan 22 10 41 10 2010	HI scaning my
13.	Jun. 168. wa 127	Tex 344 22 10 42 10 1010	IC scaling m
14	the third of	Pri Jac 22 ol 42 98 2000	10 straing m

图 7-105: DNS 监控列表



◆ 网页监控

Anysec 设备能监控并记录内网用户所有 URL GET 请求和 URL POST 请求情况: (型号不同表现形式会有不同),中端型号一般只显示最新的 200 条 URL 访问信 息,一般高端型号能够依据日期进行 URL 访问记录,并能内网 IP 来查询其所有 访问过的 URL。

● URL GET 请求:

	(SER OFF)	至M面积(mat)	网络历史记录(4871)	工程后空记录(mur)
38	17/用户	8252	EW.	101.
1.1	102 182 79 100	Tei (fas 12 10-42 1) 2000	tiptinaged op ros 5	attp://tipsinagel.go.om/tips/11022070/4
2	100:111-111-110	Fri 2m II II II II III		the free reason (see), for strand and a strand and and
	102 189.10,100	37) 3m 22 00 40 02 2000		http://www.exec.com/aaak.gfu-mittainenterationenan
	197, 188, 99, 122	111 2 m 22 10 10 11 2010	dia minamini di	ing //bg stack cu/rest20012010000341110-0200001, 1220
2	102 103 10 118	Ter 2m 27 10 42 31 1000	milates 200aufa and	Die //ophitas Millials em/W/adesp.statio estimatespil
	102 103 10 122	Tes Jun 27 10 42 17 1010	by marine B	http://log-accepts-ma/cent2041(0010040401110-ac700000ac70
121	192 166 55 107	Fri Jan 22 10 41-10 2010	fig nonginers 1	itty 7/ba anaga m/Ligt*s_iM0000r,a_e000001
81	110 188 18 122	2rt 2m 12 10 40 10 1010	be mayness a	trup //he makes m/rest.html/tocomint.col-informer, and
8.	192 155 79 137	Pri . Des 22 22 41 46 2010	news, mina and on 3	http://www.wina.com.co/if/www/if/00/with.html
10	102 108 78 117	3rt 7m 12 11 11 10 2010	int fand, sine cost	Dig Work April 1000 on infigliological-one station
11	100 100 29,107	fri Jan 22 10 41 44 (100)	ses time too on D	Htp://www.atsa.com.to/
11	102 188 38 107	Pri 2m 12 10 41 17 2012	ever merchanisment of	itty //www.augues.com/
-	110 188 19 137	fri Jus II 11 41 24 mm	ere signed and	ittp://www.aupusc.com/
++	198: 155 79,100	Per 200 22 20 10 20 2010	119,147 % 200, 3	ing June of a ministratio

图 7-106: 网页监控列表

-	10/80		194		
	101109-00110	The Dis 12 13, 14, 19 1999	inter Minute and	hild Direct Minate on Departments had	
2	101.101-108-08	the last to on the last sec-	111 Withd's Low	http://pp: mmah. on Supprisinges http:	
3	101100-000.08	The Decision of the second	page 11 may	big films as on different 30	
	101100-10-08	The line (1 of mail) come	ner berättigt ten	para chine betreatty the Constraint, and	
	100.100.100.00	Ten. No. 11. 18. 27 - # 1998.	mm balataffit (am.	date Come Beter 000 and Crater Sale Late	
4	TRUCKED SURVEY C	The No. 11 II. do by Land	see, increasing pre-	brig from manuality one spanningtown pig."	
	101100-10-08	(Tex. Per (1.04.70.00.000)	me bereinite om	ferte freme berrenten une fremengigente pte	
	140,100,100,09	The Part In call of the	men balalatie ine	http://www.bullicold.com.franchiseneg.ala	
	1.81,1.81 (1.88)	This particular on one cannot	non Statistick inst	halig from marrieller and figurerial-and pre-	
-	1011101-108-108-08	The Design of the state of the	- intrinity in	Data (read housed), one functing over \$10.	
11	101-101-1-00	the Part of the second	me billing our	http://www.maini.0001 //purfrage/wood jikp	
π.	101109-10100	the Dec 11 to the Phone	see intatation, ine	hild from according on Spectraphysic yes	
79.	101109-108-08	The Part of the State of Long-	no deineitt om	halo from berrall or from a page	
24	AND DRAMATE OF	No. 3a. 11 31 35 14 1996	- batalant ine	hits from builded, on furnetary, do	
	101100-00-00	The Deal of the rest of theme	- hundress	brig from Balarotte on Spatian tan	
	101103-101-09	The Dec 11 18 19 19 19	mer-balalaffit ing	Bits (Const. Berring Will, one chastering Starty also	
	101100-10110-	The loss of the state of pass.	ma balaisith inn	here from an and the own from the star	
	100,000 (100.00)	The real of the late of theme	sen barnalth des	haig from According and Carlingham in	

● URL POST 请求:

图 7-107: POST 监控列表



◆ 邮件监控

Anysec 设备能监控并记录内网用户所有邮件发送和邮件接收情况:(型号不同表现形式会有不同),中端型号一般只显示最新的 200 条邮件信息,一般高端型号能够依据日期进行邮件记录,并能内网 IP 来查询其所有发送和接收过的邮件。

● 已发邮件 (SMTP):



图 7-108:已发邮件列表

• 已收邮件 (POP3):

_liama	orti anno	_			61.23
	x1780*		R#A	##A	10
8	And the line of	Solar of the set	daughtin car	definity or	and and

图 7-109: 已收邮件列表

◆ 聊天监控

Anysec 设备能监控并记录 QQ 和 MSN 等及时聊天软件的使用情况,对于 QQ 软件, Anysec 能实时获取该 IP 用户所使用的聊天 QQ 号以及查看当前 QQ 是否在 线。对应 MSN 软件, Anysec 设备不仅能获取该 IP 用户的 MSN ID 号,并且能记 录 MSN 双方的聊天记录。



● QQ 监控:

REAL		3							
18	#15	ALCONN.	84	#10°	SHEET)	ALMER T	BURGET.	244.4	
	10.101-014	Sec. (44) 11 10 10 21 200		18.18.10.0	1000	316 22 19 24	1010		
	officers.	The loss of all of all all all	100	1. 100.100.000.000	1000	April 101 (11.00)	100	•	

图 7-110: QQ 监控列表

● MSN 监控

-	-				 			4 - 4
	#16.4	84.2010			 in the second se	Distant -	Bara -	81
	have the second	No. No. 12 / 7, 41 (2007)	- 33	10.00.00.00	10 To 30 H	1943		20

图 7-111: MSN 监控列表

◇ P2P 监控

Anysec 设备能够对目前流行的 P2P 下载工具 BT、电驴以及迅雷实时报告,管理员可以通过该功能及时获取内网 IP 用户对 P2P 软件的使用情况。

● BT 监控



图 7-112: BT 监控列表



● 电驴监控

HAR	 AR.				4++
- 19	 Are.	A 2 4 4	1011	Ants	-

图 7-113: 电驴监控列表

● 迅雷监控

		-				
1.88	-	BPE.	A PAN	1446	ANTS	84

图 7-114: 迅雷监控列表

◇ 娱乐监控

Anysec 设备能对 QQ 音乐及 QQ 游戏进行实时监控。管理员能通过该功能获 取当前 IP 用户的 QQ 音乐和 QQ 游戏的使用情况。

● QQ 音乐





图 7-115: QQ 音乐监控列表

● QQ 游戏



图 7-116: QQ 游戏监控列表

♦ FTP 监控

Anysec 设备能够监控内网 IP 用户使用 FTP 协议进行文件上传下载情况。



图 7-117: FTP 监控列表

Э 日志审计

Anysec 设备提供了多种日志,您可以通过查看日志信息获取系统的各种日志:



◆ 系统日志

200	-			
			**	
	And they be the life and the	1.1	NAMES OF BRIDE	PHERE EX
	And Name in case of the party	2.2	and a strategy of the state of	229 Converter, plat
	ful flag 25 (2) (2) (2) (20)	4.4	and the second sec	MEL BOAR Land ARCHES LANDS ST. PROBATION OF ST.
4	Not they of the lot of some	0.0	Walter I again the say	Print
	And they do not be all press	6.6	Witness I append that an affilit	ten Wilson 2
1	that they let it. 10 to prime	8.8	NAME OF BRIDE	wryna Xe
	the Real of the Local Distance	4.8	Der register offen er	K282 819240.068
4	Ber Was 20, 20, 14 (M 1998)	11	a comparation of the second seco	Miles Bridge and Allerian Longing and Palacets (100 per st.
	Northeast of the second party		WHERE I suprai 1995, and	Reve
-	And And in case of the local division of	14	Without a new loss of giving	Inc States
	No for the second		1.001.000.000	antista i X.A.
	in to 21 10 10 10 1000		DOWNERSON .	ADDI A-MARINARY
	Day Rep 14 (2) Perch 2000		an realized Post in	and all and address on the S. Stars in the S.
-	Ten Way 10 12 10 10 10	8.8	Raine and the same	Range
-	The Rey Of the Section and	6.6	Show I again that applied	netters a
-	the Real of String on Links	11	STREET OF STREET	WTERR-X4
	And they in the lot of the		AND REAL PROPERTY AND ADDRESS OF THE PARTY OF	Man reader to
-	Real Prop 12 and 18 and 1988		In the Real Property lies in the local division of the local divis	Na Latita
	Bur Bar Martin & print			ORMANDAL CO.

图 7-120: 系统日志列表

◇ 防火墙日志

ARTER	2			 	 		
10		alk of the	ALC: NO.	 Batter .	 BHIL/BR	Hereco/eses	

图 7-121: 防火墙日志列表

◇ VPN 日志

● 点点通日志



图 7-122: 点点通日志列表



● PPTP 日志

-	and the second	(.anavana.)		
**	100	1.1	2.66	

图 7-124: PPTP 日志列表

● IPSEC 日志



图 7-123: IPSEC 日志列表

● SSL 日志



移动客户端日志



图 7-124: 移动客户端日志列表



● 操作日志

-	-					4
24				848		84
	Stat. Bay (\$150-10), \$10.	4.8	-	8738		
	And Page 21 (2) 19, 41	12		HALLER.		
	No. 94 21 22 18 10	- 6.8		H-BR	42	
	114 84-11 2-1 11	22		计算子自己和信托	61 29	148
	Test Ray (2) (2) (6) (2).	6.8	where	PRODUCT CONTRACTOR	40 94	
	that they go to be set.	2.2	other	specification in the second se	41	
	Aug. 20, 20, 20, 40	8.8.		Ares	63	
	The Res of Lines. Inc.	11.0		11-24		
-	The Report of the life		-	300 2 2 5 4 C	45	
	The Rep 10 18 (00 HB)	11		1.128		
	The Res 21 14 14 141	4.8		N788	63	
	The Ref 11 10.01 10.	10.00		21-24	- 61	
	ALC: No. 10, 10, 10, 10, 10,			1.188	4.0	
14	An Au 21 18 18 19.			Broathalty BR	4.0	
-	The Bal 21 10 10 10	1.0		1111112	63	
	Pro Bar 21 (0) (0) (0)	11		Million March 1997	80	
	Ro. by 12 11 12 12	12	other	HALLER .	-	
	A	12		April 1 Per	1.48	
	The Res Of Strike we	1.0	1000.0	8788	100	



◆ 日志配置

Anysec 设备支持本机日志和远程 syslog 日志

白耒淮常	日志夜竖
◎ 本机日志 ● 远程日志	
日志服务器13	御定

图 7-125:日志设计界面

若选择远程日志,请先确认远程 SYSLOG 服务器进程是否已启动。



第八章 Console 配置

ANYSEC 系列产品支持 Console 配置方式,本章介绍如何使用 Windows 系统超级终端控制台程序配置设备。

Э 连接

Console 配置方式硬件接线图示:



图 8-1: Console 配置连接图

以 Windows XP 为例。在"开始""程序""附件""通讯""超级终端", 启动超级 终端。

1、 新建连接, 新建 anysec, 如下图示:



连接描述	? X
新建连接	
9	
输入名称并为该连接选择图标:	
图标 (L):	
🔊 🙈 🔈 🚾 👧 🔂	
	>
· 确定 · 取ì	۴ <u> </u>

图 8-2: 新建连接名称设置-1

2、 选择正确的 COM 口,根据实际连接接口,选择正确的 COM 口(连接计算机使用的串口),如下图示:

连接描述			? ×
新建连接			
◇ ☆ ↓ 2 む エン シン	网标		
名称(图):	ESTAD -		
anysec			
图标(L):			
	MCI	(aga	
	-9	W	13
			<u> </u>
			344
		開定	7月

图 8-3: 新建连接名称设置-2

3、 COM 口属性配置。如下图示:



毎秒位数 (B):	9600	*
数据位 (电):	8	*
奇偶校验 (P):	无	*
停止位 (2):	1	~
数据流控制 (2)	: [无	*

图 8-4: 调整 COM 口属性界面

● 基本配置

系统正常引导启动后。初次登陆配置,在提示登陆处输入缺省账号: ANYSEC Login:admin

Password:anysec (密码输入为隐藏状态,无显示) 成功登陆后,显示如下:





图 8-5: Telnet 登陆界面

输入 # 回车, 显示主菜单, 显示如下:

			The second	-
Ma	leane to Anyree UPM System			1
 Boysec-No 	tuark (ShenZhon) Ce., Ltd Copyrigh	e -		1
An Leoner, and a	te 11 in Man Jan 25 18:23:43 UTC 2	PI D		
sinin#> #	the first the time is a state of the state o	419		
whey ier:	Exter Rebaving Module			
11	Clear the acress			
Lagnose	Ester the Diagouse Module			
ixecute	Bater Execute Models			
suit	Exit this GLI session			
trevel1	Ester Firesall Module			
ler 1 p	Display an everyiew of the GLI sp	ntas:		
listory	Dioplay the current provion's can	mond line history		
ley	Enter Log Madale			
logent	Lagout of the current CLI secoion			
retmonithr.	Eater Networiter Module			
an treate la	Eater Hetwark Madule			
neval1	thos current reaning configuratio			
getan.	Dater Eysten Medula			
LOPP	Tangen Hills Made 1			
(pas)	Dater orm housis			
delait's H				

图 8-6: Telnet 下配置界面


第九章 常见问题解答

本章列举了部分常见的问题。更多 FAQ,敬请参考 www. any sec. com。

▶ 忘记密码怎么办?

ANYSEC 系列产品在后面板有 Reset 键, 按住几秒钟后, 前面板 system 第四盏 灯亮起, 则登陆地址、用户名、密码会恢复为默认。也可以通过串口登陆设备并重 启设备, 在重启过程中按"i"键, 用户名、密码同样会恢复为默认。

➢ 如何查看当前设备接口状态及其 IP 地址?

在 WEB 管理界面,进入"系统管理"----"网络管理"----"接口"可以看 到各个接口的 IP 地址及连接状态等信息了。

如何确认自动隧道已成功建立?

使用点点通时,点击 "VPN 管理" —— "点点通" —— "隧道监控" —— "测 试"。如果隧道建立成功测试结果正常。

- ➢ 局域网不能上网如何处理?
 - 1. 请先查看电脑到网关之间是否通畅。

2. 如果通畅查看面板的 WAN 和 system 指示灯状态:如果 WAN 等不亮或 system 灯为左灯灭,右灯闪烁,此时为外网故障。请检查 Anysec 外网线连接是否正常; 重启 Anysec 设备或 Modem。如果还不能恢复正常,请使用单台电脑上网是否正常,如果不正常,请联系运营商解决。

▶ 能上网但不能和其他节点的主机或服务器通信,该如何处理?

A 点击 Web 管理界面的 "VPN 管理" - "点点通" - "隧道监控" 查看隧道 是否正常。

- ➢ ADSL 无法拨号上网
 - 1、检查线路是否松动
 - 2、检查 ADSL 账户和密码是否填写正确
 - 3、部分地区的 ADSL 用户,在终端设备突然断电后,不能马上拨号。需要等待 一段时间才能重新连接。
 - 4、确认 Modem 是处于路由模式还是透明模式。Modem 如是路由模式请修改为透 明模式,由 Anysec 设备进行 PPP0E 拨号。
- ➢ ADSL 线路很不稳定,常常断线怎么办?

当前 ADSL 一般使用 PPPOE 拨号,拨号成功后拨号程序会不断地发送 LCP (链路控制协议)包来维护 PPP 连接。如果 ADSL 线路过长,或者线路质量不好,ADSL Modem故障等,都容易导致 LCP 数据包发送和接收异常,造成连接中断。

- 1、检查内网是否有病毒造成大量往外发包,或者内网有使用 BT 等 P2P 工具下 载造成上下行数据量较大,或者内部计算机较多正常访问量很大, ADSL 不能满 足带宽要求等。这些情况都容易导致 ADSL 出现断线重拨。
- ADSL 线路本身不稳定,容易断线重拨。可以使用电脑拨号进行验证。线路问题请及时联系线路服务商获得支持。

● 故障处理流程

当内网 PC 无法连接 Internet 时,首先检查设备是否已正常连接 Internet,处理流 程参考如下:





图 9-1: 设备故障处理流程图



附: 点点通配置实例

本章将以实例讲解点点通配置过程,本实例是在 ANYSEC 设备通过智能安装向导配置后, 设备已经正常运行,进行单独配置点点通 VPN 互联模块为目的。分为中心点和分支节点 两部分介绍。

○ 客户背景介绍

● 总部中心点:

ANYSEC 设备作为网关,通过固定 IP 上网; 内网网段: 192.168.1.0,网关地址: 192.168.1.1,掩码: 255.255.255.0。

● 分支节点 A:

ANYSEC 设备作为网关,通过 ADSL 上网; 内网网段: 192.168.2.0,网关地址: 192.168.2.1,掩码: 255.255.255.0。

○ 总部点点通管理平台配置

1、 点击 "VPN 管理" —— "点点通" —— "设备管理",如下图所示



图附−1



点击右上角"新建"添加设备,现将总部中心点设备添加至点点通平台。如下图所示:

2室	隧道监控	设备管理	<u>连接管理</u>	在线设备
		4982	新建築	
		19 & ID	1000	
		(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)		<u></u> 1
		联网模式	静态公阿IP	
		即把址	123. 123. 123.	123
		内网口P	192, 168, 1, 1	
		在线生存期	300	(120-3600秒)
		联系人	工程师	
		电话	13510693536	
		备注	总部设备	
		确定	取当	
		100 C		

图附-2

注意: 联网模式请根据实际情况填写, 拥有固定 IP 上网方式, 请选择静态公网 IP; ADSL 上网方式或接在内网交换机下时, 请选择"动态公网 IP 或 NAT 后"。此处 根据客户实际情况, 我们选择"静态公网 IP", 并将公网 IP 地址填入"IP 地址"栏 (动态公网 IP 没有此项)。**内网口 IP:** 指该设备所在网络内网网口 IP 地址。

3、 点击"确定",系统会提示是否继续为该设备进行隧道,点击"确定"。如下图所示:

配置	隧道监控	设备管理	连接管理	在线设备		
		设备总部新建成	功,是否继续为	该设备进行隧道子网第	定义?	
				-		
			佣定	取 洞		



图附−3

4、点击"确定"后,进入隧道子网列表,点击右上角"新建"图标,添加隧道子网, 如下图所示:

松田	築業調整	RATE	法政策提	在线设备		ŭ
ID	子网名		10		應码	编辑

图附−4

5、点击"新建"后,填写子网名(任意填写), IP 地址:该设备内网网段,如 192.168.1.0, 子网掩码填写:255.255.255.0。如下图所示:

※王 職業協行		雪澤 在鉄设备
	子网名	
	1Pt@t <u>it</u>	192.168.1.0
	网络掩码	255, 255, 255, 0
	机度	取 消

图附−5

6、 点击"确定",进入设备管理列表,列表中显示已添加过的设备。如下图所示:

	#	新油市 位	() () ()	刘庄王和 1	TROB			6
89	12 # 8	2条10		脉搏子网	联网万式	在线生存 期(物)	条注	-
1	読品	1000	192.168.1.1	192.168.1.0/255.255.255.0	観念公園の	300	总部设备	
	64	1000	192.100.1.1	199.108.10955.255.255.2	# C1340+	300	ALC: NO	



图附−6

7、点击右上角"新建"再继续添加设备,现将分支节点设备添加至点点通平台。如下 图所示:

を用	能進溫程	设备管理	连续管理 在统设备
			新建设备
		设备名	北京分部
		设备ID	1001
		通讯密码	*****
		鉄時模式	动药公网1P或NAT设备后 •
		内网门户	192, 168, 2, 4
		在线生存期	300 (120-3600 (9))
		默系人	北京門智
		电透	13713867534
		备注	北京分公司两营
		ME	IX H

图附−7

8、点击"确定",系统再次提示是否进入隧道子网配置,点击"确定",新建该设备的隧道子网,填写子网名(任意填写),IP地址:该设备内网网段,如192.168.2.0,子网掩码填写:255.255.0。如下图所示:

	造用要查 在线设备 建水型分积设备整道子000
子网名	VPS
即把社	192, 168, 2, 0
詞络補知	255, 255, 255, 0
	e 17 H
and the second s	

图附-8

9、 点击"确定",进入设备管理列表,列表中显示已添加过的设备。如下图所示:



60	×	1. 通道规		建建管理 3	石炭设备			
序号	设备名	设备的	PARICIP	建银子网	联网方式	在戦生存 期(秒)	6 /2	-
1	85.88	1000	192,168,1.1	1921081.0955.255.255.0	#市台市中	300	息相段番	鲍之曾
12	北京分割	1001	192.168.2.1	192.168.2.0/255.255.255.0	边态达HIDPSDAFT 设备和	300	北京分公司 (20世	10 2 C

图附-9

10、 点击"连接管理",进入设备列表后,点击"总部"设备后面编辑选项中的"修 改连接策略",如下图所示:

配置	建装装控 设备管理	在田田田 在线设备	
(D	088	能過数	1941 - C
1,	日田	0	
2	北原分别	0	Q 2

图附-10

11、 点击"修改连接策略"后,进入编辑界面,将左侧列表中的"北京分部"选上, 点击中间的"向右添加"按钮,将"北京分部"添加至"总部"设备的连接设备列 表中。如下图所示:



	明네크	腺藥酶	
设备名 (A)部			
可互联设备		已选设备:	
		は出来は単語	
	14		-
	-	_	

图附-11

12、 点击"确定"后,返回连接设备列表界面,在此处可以看到每台设备的连接隧 道数。如下图所示:

IN M.	董道斯控 设备管理	高振智慧 花线公泰	
ID	设备名	睡眠的	新聞
1	陸相	1	\$P
2	北原分司	1	44 (A

图附−12

13、 设备添加完成后,下一步将激活点点通策略中心,点击"配置",填入总部中心 点的设备名、设备 ID、通讯密码、隧道策略寻址方式、策略中心地址,并勾选"现 在激活"选项。如下图所示:



 単花校 空茶管理	法推荐规	在线设备		
	设备起	T.		
设备名	总部			
设备ID	1000			
通用密码		•		
薩邊策略寻址方式 ● 通过公司印度 1	8名寻社			
 通过SecROSIX 	國平台寻址			
策略中心地址	123.123.11	13.123		
上艰廉略中心地址			E3	
現在激活	101			
	備臣			

图附-13

点击"确定",系统会提示"上线成功"。至此,点点通中心点设备配置完成。通过 点点通"隧道监控",可以测试隧道是否建立成功;通过"在线设备",可以查看所 有设备是否在线、所有设备公网 IP、进行远程管理、下发策略等。如下两图所示:

D	12:010		诸语方式	中醫設量	######	当相状	-	10.75
1	1000	devial	高洲这種		192.168.118.0455.255.255.0	1		69
	Tion	devent	-		192104002552552550	-	. Aitk	4
3	1004	devia5	直接运行		100.168.86.0455.055.055.0	18	制成	-
4	1996	deviad	高短信禄			-	AUR	-





图附-15

Э 分支节点配置:

点击 "VPN 管理" —— "点点通" —— "配置"。如下图所示:



松寨 装 用具作 交易管理	连续增增 石线设备 设备配置	
没参考 没参切	北京(計画) 1001	
通訊服料 簡濃東絡寻址方式。 ● 通过公開P版場 ● 通过公開P版場	1名非社 後平台非社	
服務中心地址 上級開路中心地址	123, 123, 123, 123	
现在潮沽	國 (1)	

图附-16

填写由总部下发的设备名、设备 ID、通讯密码(即中心点点点通管理平台添加 在线设备时,填写的信息),此例中应填入设备名:北京分部,设备 ID: 1001,设备 密码: ******。

隧道策略寻址方式: 当总部为固定 IP 或域名时,填写 IP 或域名,当总部使用 SecROS 网络平台寻址时,填写我司授权给中心点设备的 SecROS 简域即可。

勾选"现在激活",点击确定。如果信息填写正确,系统会提示上线成功;如果 信息填写错误,系统会提示"隧道策略获取失败,请检查设备主机名、设备 ID、密 码以及策略中心设置是否配置正确!"。

设备成功上线后,可以在隧道监控中查看隧道连接状态,并可测试隧道连通性。

注意: 当总部中心点没有固定 IP 时,推荐使用我司拥有自主知识产权的 SecROS 认证平台进行寻址互联,更加稳定、安全、快速。若采用点点通平台,仅需在隧道策略寻址方式项,选择"通过 SecROS 网络平台寻址",在"策略中心地址"中,填入由我司授权给您的"简域名称"即可。